GFI MailEssentials 2010

Getting Started Guide

By GFI Software Ltd.

http://www.gfi.com
info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI Software Ltd.

GFI MailEssentials was developed by GFI Software Ltd. GFI MailEssentials is copyright of GFI Software Ltd. © 1998-2010 GFI Software Ltd. All rights reserved.

GFI MailEssentials is a registered trademark and GFI Software Ltd. and the GFI logo are trademarks of GFI Software Ltd. in the Europe, the United States and other countries.

Version ME-GSG-EN-1-02.009

Last updated: March 3, 2011

Contents

1 Introduction 1

1.1 About this manual 1
1.2 Terms used in this manual 2
1.3 Licensing 2

2 How does GFI MailEssentials work? 3

2.1 Inbound mail filtering 3
2.2 Outbound mail filtering 4

3 Installation for Microsoft Exchange 2003 5

3.1 Introduction 5
3.2 System requirements 5
3.3 Important settings 6
3.4 Installing on Microsoft Exchange Server 2003 7
3.5 Installing on an email gateway or relay/perimeter server 15
3.6 Installing on Microsoft Exchange 2003 cluster 28

4 Installation for Microsoft Exchange 2007 & 2010 45

4.1 Introduction 45
4.2 System requirements 45
4.3 Important settings 46
4.4 Installing on Microsoft Exchange or SBS server 47
4.5 Installing on an email gateway or relay/perimeter server 54
4.6 Installing on Microsoft Exchange Server 2007 clusters 64

5 Installation for Lotus Domino 67

5.1 Introduction 67
5.2 System requirements 67
5.3 Important settings 68
5.4 Installing on gateway servers for Lotus Domino 69

6 Installation for SMTP Servers 83

6.1 Introduction 83
6.2 System requirements 83
6.3 Important settings 84
6.4 Installing on gateway servers for SMTP Servers 85

7 Post-install actions 99

7.1 Test your anti spam system 100
7.2 GFI MailEssentials Configuration 101

8 Uninstalling GFI MailEssentials 103

8.1 Introduction 103

9 Troubleshooting and support 105

9.1 Introduction 105
9.2 Troubleshooting: Installation issues 105
9.3 Knowledge Base 106
9.4 Web Forum 106
9.5 Request technical support 107
9.6 Build notifications 107
9.7 Documentation 107

10 Appendix - Installing MSMQ 109

10.1 Windows Server 2003 109
10.2 Windows Server 2008 111

11 Glossary 113

12 Index 117

1 Introduction

1.1 About this manual

The scope of this 'Getting Started Guide' is to help you install and run GFI MailEssentials on your network with minimum configuration effort. It describes:

1. The various environments and email infrastructures supported by this product

2. Guides you through the respective installation procedure

3. Walks you through the key steps needed to get the product running on default settings.

Manual structure

The sections in this manual are 'self contained' and are designed to guide you through the sequence of steps needed to:

1. Identify product prerequisites applicable to your network

2. Prepare your environment for product installation

3. Install/upgrade GFI MailEssentials

4. Configure, test and run the product.

Follow the instructions for your type of network using the appropriate section in this manual. Where applicable each section contains information related to installing GFI MailEssentials on the same server as your mail server, on a mail gateway or relay/perimeter server or in a clustered environment.

Administration and Configuration manual

Detailed administration and configuration guidelines are provided in a separate manual called **GFI MailEssentials Administration and Configuration manual** which is installed with the product or separately downloadable from the GFI web site:

http://www.gfi.com/mes/manual

This Administration and Configuration manual complements this Getting Started Guide by providing more detailed information on how to use and customize the features provided in GFI MailEssentials (e.g. tweaking of anti spam filters).

1.2 Terms used in this manual

The following terms are used in this manual:

- **“NOTE:”**
  - This provides additional information and references essential to GFI MailEssentials’ operation.
- **“IMPORTANT:”**
  - This provides important information such as warnings and cautions that advise of potential issues commonly encountered.

For any technical terms and their definitions as used in this manual refer to the Glossary chapter.

1.3 Licensing

Information on licensing is available on:

http://www.gfi.com/products/gfi-mailessentials/pricing/licensing

2 How does GFI MailEssentials work?

2.1 Inbound mail filtering

Inbound mail filtering is the process through which incoming email are filtered before delivery to users.

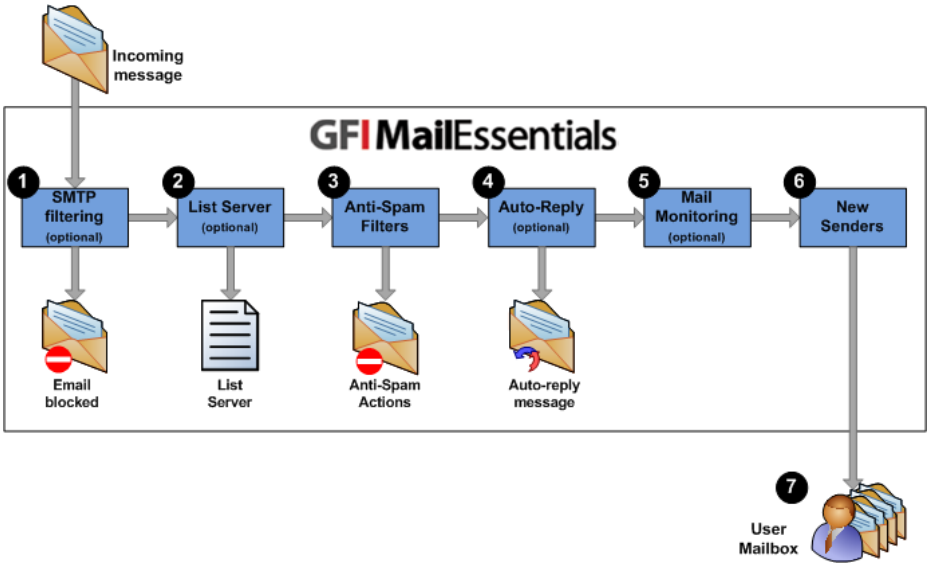


Figure 1 - Inbound mail filtering

When an email is received:

1 SMTP level filtering (Directory Harvesting and Greylist) is executed before the email body is received.

2 When the email is received, it is checked to see if it is addressed to a list in the list server. If the email matches a list, it will be processed by the list server.

3 The incoming email is filtered using all the spam filters. Any email that fails a spam filter check is sent to the anti spam email actions. If an email goes through all the filters and is not identified as spam, it then goes to the next stage.

4 If configured, email is next archived to the archiving database.

5 If configured, auto-replies are next sent to the sender.

6 If configured, email monitoring is next executed and the appropriate actions taken.

7 The new senders filter is now executed.

8 Email is sent to the user's mailbox.

2.2 Outbound mail filtering

Outbound mail filtering is the process through which email sent by users within a company is processed before it is sent out.

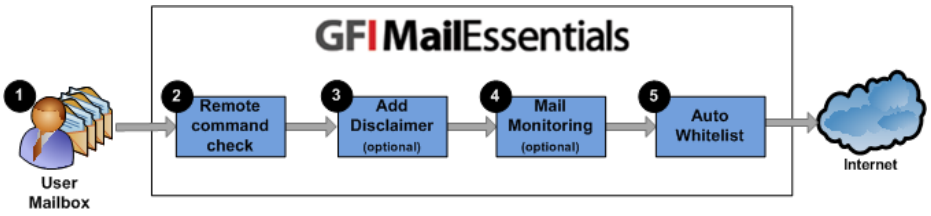


Figure 2 - Outbound mail filtering

1 User creates and sends email.

2 Remote commands check executes any remote commands in email if any are found. If none are found, email goes to the next stage.

3 Email is next checked to see if it should be archived. If archiving is enabled, email is saved in the archiving database.

4 If configured, the applicable disclaimer is next added to the email.

5 Email is checked for any mail monitoring which may apply and action is taken according to any rules configured.

6 If enabled, auto-whitelist adds the recipient's email address to the whitelist. This automatically enables replies from such recipients to go to the sender without being checked for spam. After this check, the email is sent to the recipients.

3 Installation for Microsoft Exchange 2003

3.1 Introduction

GFI MailEssentials installation depends on how your network is configured for Exchange 2003. You can install this product on:

- **The Microsoft Exchange 2003 server:** This setup is typically used to filter email spam on the mail server that is configured to receive emails directly from the internet.
- **The SBS 2003 server:** This setup is used to filter email spam on the SBS 2003 server, which uses Microsoft Exchange to receive emails directly from the internet.
- **The mail relay server:** This setup is commonly used to filter spam in distributed email infrastructures., especially those running a DMZ. In this environment a dedicated machine (also known as a gateway/perimeter server is set to relay emails to another mail server (running Microsoft Exchange). GFI MailEssentials is installed on the gateway/perimeter server so that email spam is filtered before reaching the mail server. This setup reduces network traffic, email storage and processing requirements on your mail server.
- **Microsoft Exchange Server & IIS Clusters:** This type of installation is commonly used to filter spam within environments where clusters are used as disaster prevention and recovery.

3.2 System requirements

3.2.1 Software

Supported operating systems

- Microsoft Windows Server 2008 Standard/Enterprise
- Microsoft Windows Server 2003 Standard/Enterprise (x86 or x64)
- Microsoft Small Business Server (SBS) 2003 (SP1)

Supported mail servers

- Microsoft Exchange Server 2003 (SP2)

Other components

- Microsoft .NET Framework 2.0
- Microsoft XML core services: This is required by the GFI

MailEssentials reporter to enable anti spam report generation. For UK/US English OS this is installed automatically by GFI MailEssentials. For other languages, this can be downloaded from:

http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- Microsoft Virtual Server cluster group resource with a physical disc cluster. This is required ONLY for environments running Microsoft Exchange 2003 clusters. For more information refer to:

  http://technet.microsoft.com/en-us/library/bb124318(EXCHG.65).aspx
- Microsoft Message Queuing Services.
- Internet Information Services (IIS) SMTP service.
- Internet Information Services (IIS) 6 or 7 WWW service, when using Quarantine or Archive Web Interface.
- Microsoft Data Access Components (MDAC) 2.8 - included by default on Windows Server 2003 or later. This can be downloaded from:

  http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en

3.2.2 Hardware

Processor

- **Minimum:** Intel Pentium or compatible 1 GHz 32-bit processor
- **Recommended:** x64 architecture-based server with Intel 64 architecture or AMD64 platform.

Memory

- **Minimum:** 1GB
- **Recommended:** 2GB RAM

Physical Storage

- **Minimum:** 500MB for installation, 2GB for execution.
- **Recommended:** 500MB for installation, 4GB for execution

3.3 Important settings

3.3.1 Antivirus and backup software

Antivirus and backup software may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials.

Disable third party antivirus and backup software from scanning the following folders:

x86 installations (32-bit)	X64 installations (64-bit)
<..\Program Files\GFI\MailEssentials>	*<..\Program Files (x86)\GFI\MailEssentials>*

<..\Program Files\Common Files\GFI>	<..\Program Files (x86)\Common Files\GFI>
<..\Inetpub\mailroot> If installed on a gateway machine.	
<..\Program Files\Exchsrvr\Mailroot> If installed on the same machine as Microsoft Exchange 2003.	

3.3.2 Firewall port settings

Configure your firewall to allow the following port connections. These ports are used by GFI MailEssentials to connect to GFI servers:

- **DNS (Port 53)** - Used by anti spam filters (IP DNS Blocklist, Sender Policy Framework, Header Checking).
- **FTP (Ports 20 and 21)** - Used by GFI MailEssentials to connect to 'ftp.gfisoftware.com' and retrieve latest product version information.
- **HTTP (Port 80) -** Used by GFI MailEssentials to download product patch and anti spam filter updates (i.e. SpamRazer, Anti-Phishing, and Bayesian anti spam filters) from the following locations:
  - 'http://update.gfi.com'
  - 'http://update.gfisoftware.com'
  - 'http://support.gfi.com'
  - 'http://db11.spamcatcher.net' (GFI MailEssentials 14 or earlier)
  - 'http://sn92.mailshell.net' (GFI MailEssentials 14 SR1 or later)
- **Remoting (Ports 8021)** - Used in the latest builds of GFI MailEssentials for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server.

  NOTE: Ensure that no other applications (except GFI MailEssentials) are listening on port 8021.
- **(OPTIONAL) LDAP (Port 389)** - Used by GFI MailEssentials to get email addresses from SMTP server. Only required if the server running GFI MailEssentials does not have access/cannot get list of users from Active Directory e.g. in a DMZ environment or other environment which does not use Active Directory.

3.4 Installing on Microsoft Exchange Server 2003

3.4.1 Upgrade from earlier version

If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

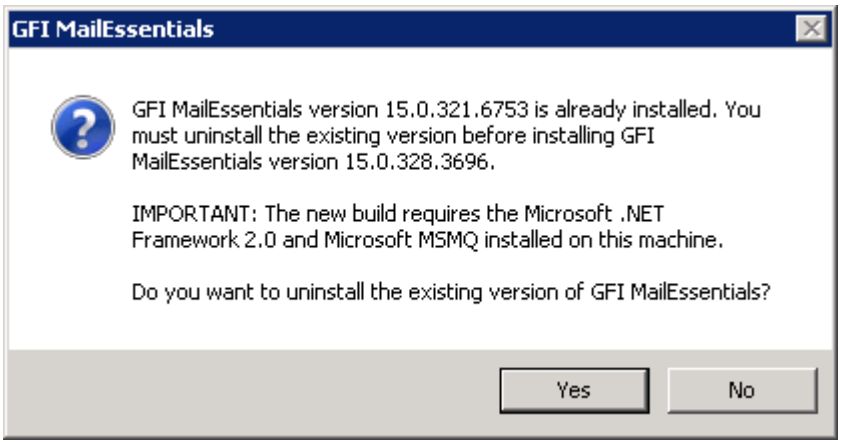
Important notes

- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.

- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com
- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. No data will be lost.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 1 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to New installations section below.

3.4.2 New installations

Pre-install actions

No pre-install actions or configurations are required.

Important notes

1. At the end of the installation process, GFI MailEssentials will restart Microsoft Exchange Server services. This is required to allow GFI MailEssentials components to be registered and started. Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.

2. Before starting installation, close any running Windows applications.

Installation procedure

1. Logon to the Microsoft Exchange Server machine using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or

mailessentials2010_x64.exe (64-bit install) accordingly.

3. Select installation language and click **Next**.

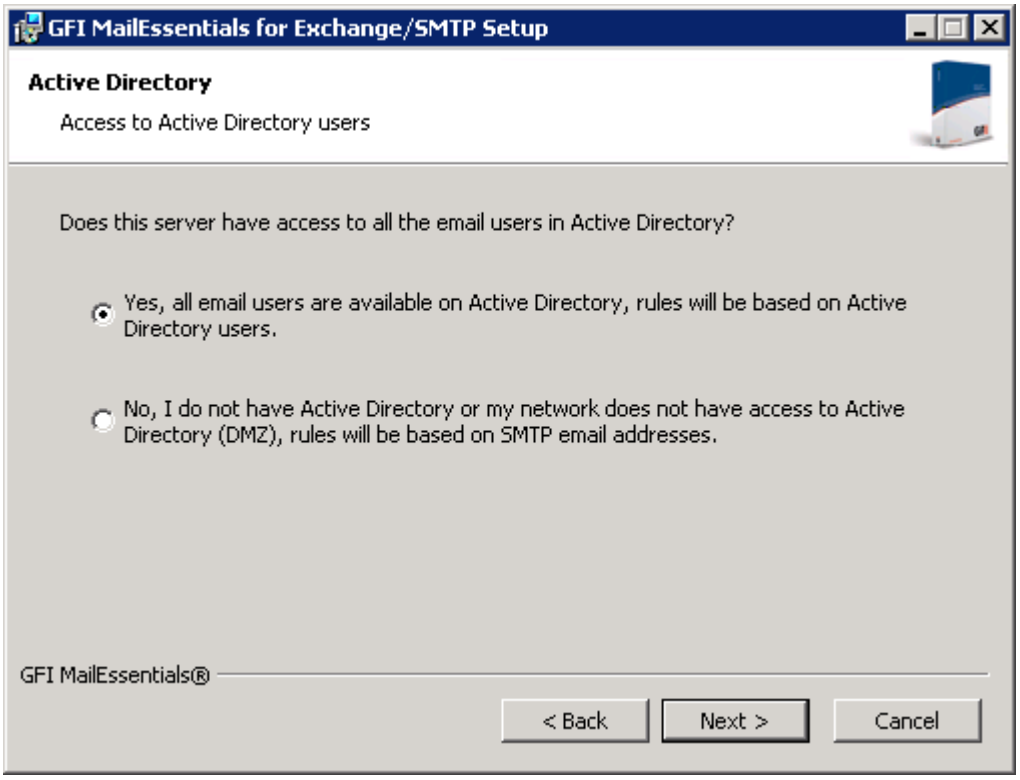
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

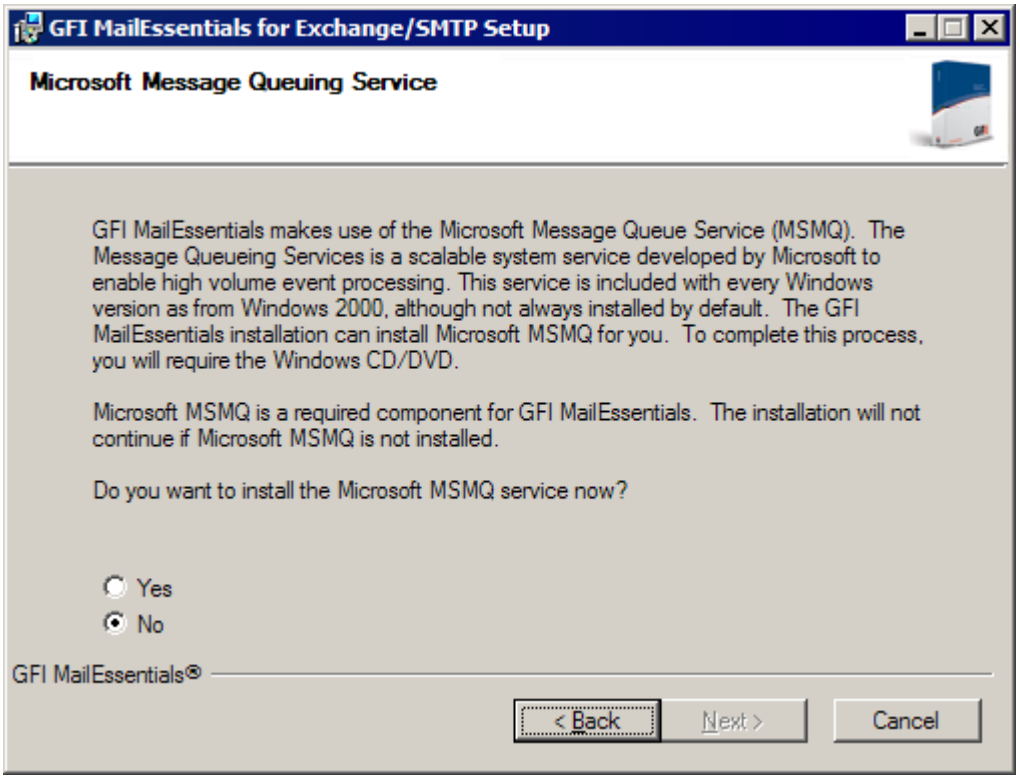
7. Specify user details and enter license key. Click **Next** to continue.

8. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 2 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue.


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 3 - Installing Microsoft Message Queuing Service

10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

11. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service.

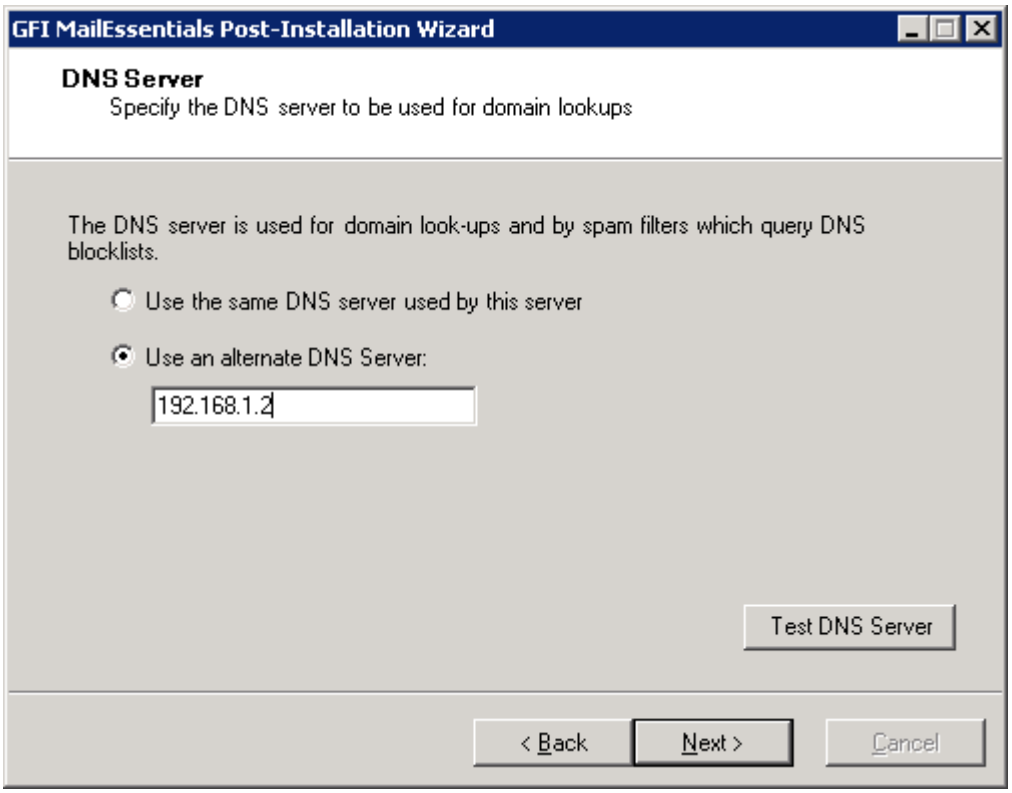
  IMPORTANT: Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.

- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

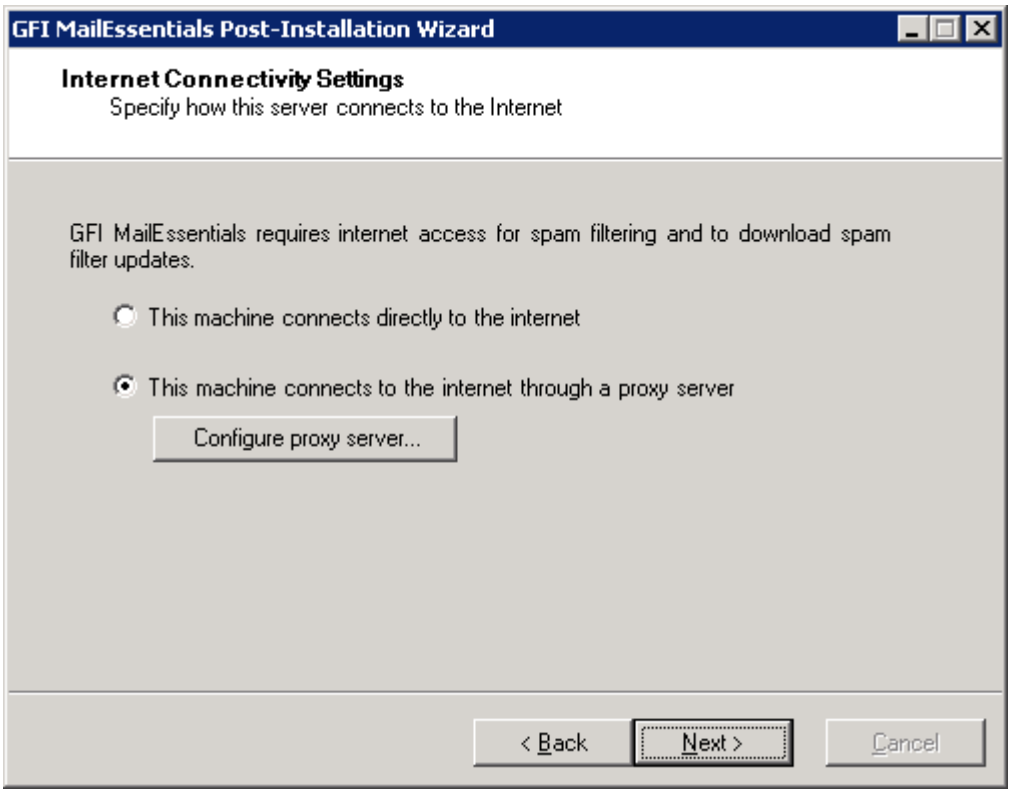

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 4 - DNS Server settings

2. In the **DNS Server** dialog, select:

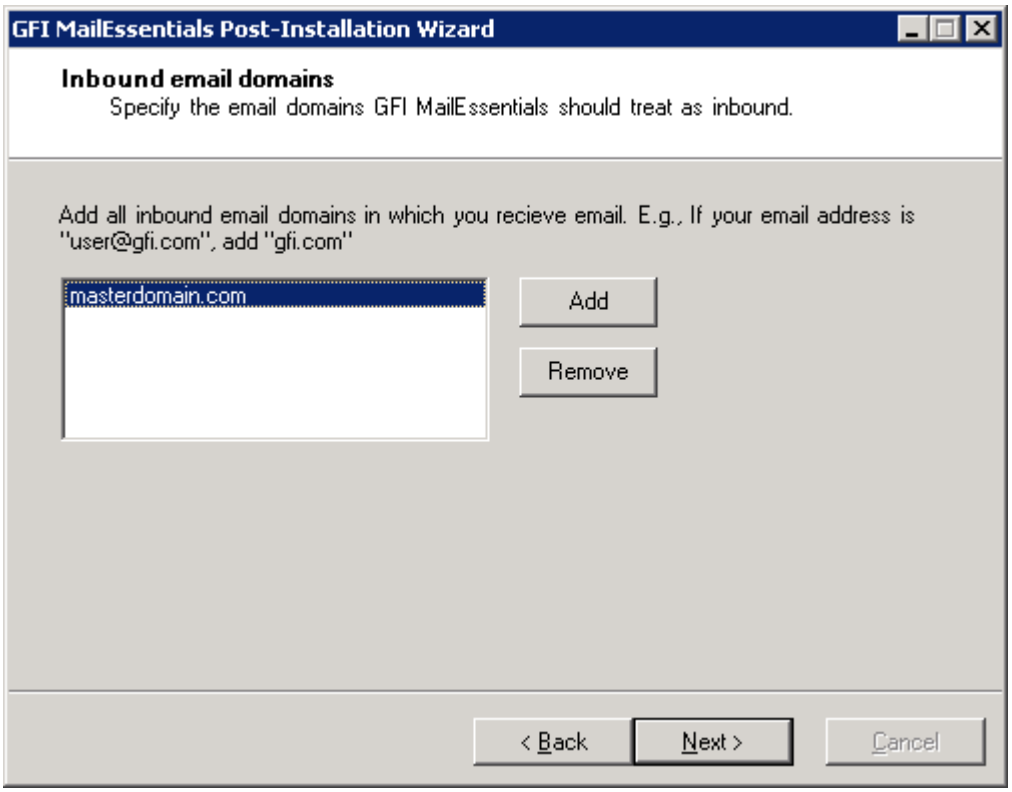
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 5 - Internet connectivity settings

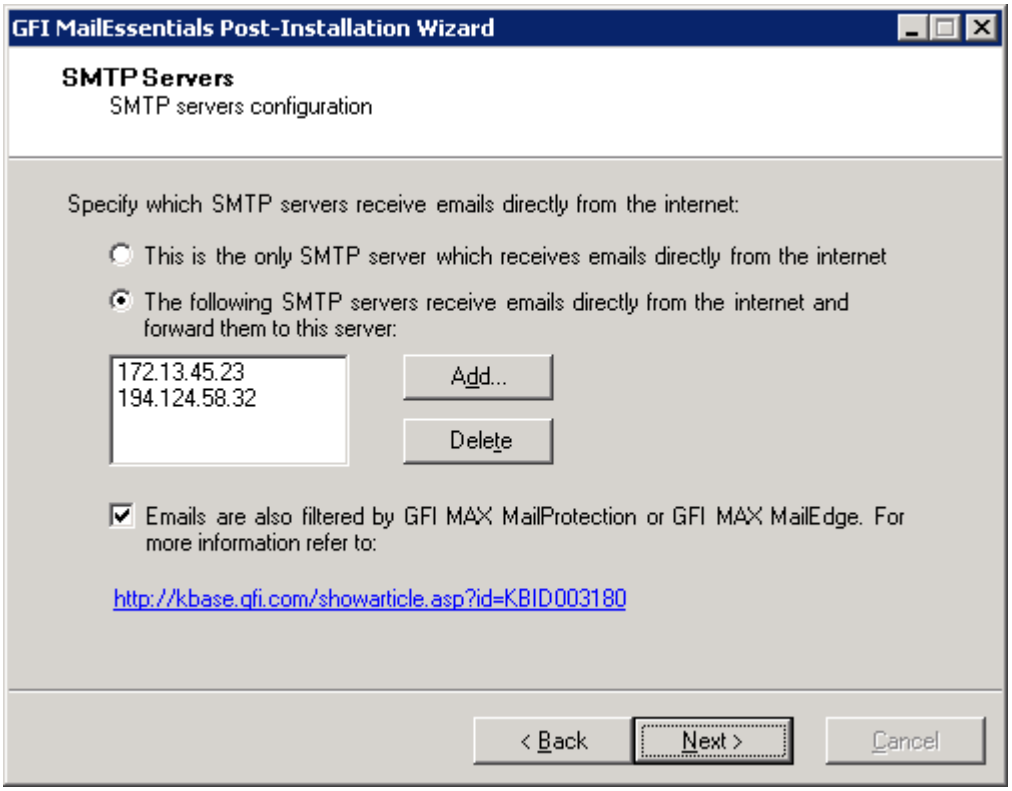
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 6 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 7 - SMTP Server settings

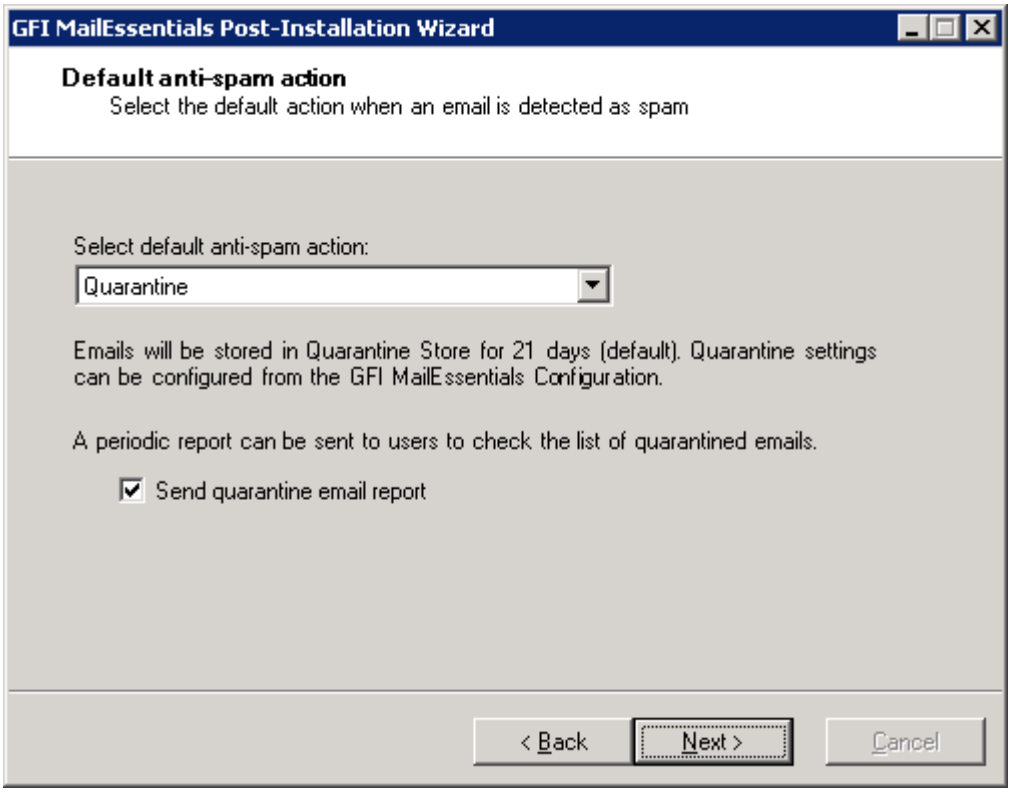
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 8 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

3.5 Installing on an email gateway or relay/perimeter server

Introduction

GFI MailEssentials can be installed:

- On a perimeter server (e.g. in a DMZ)
- As a mail relay server between the perimeter (gateway) SMTP server and the recipients' inboxes.

Both setups enable you to reduce unnecessary email traffic by using your Active Directory resources (at a perimeter/gateway server level) to drop connections for non-existent email recipients in incoming email. This helps counter spamming techniques such as Directory Harvest Attacks (a brute force type of attack used by spammers to find valid/existent e-mail addresses at a domain). This structure stops the majority of Spam from arriving at your Microsoft Exchange server.

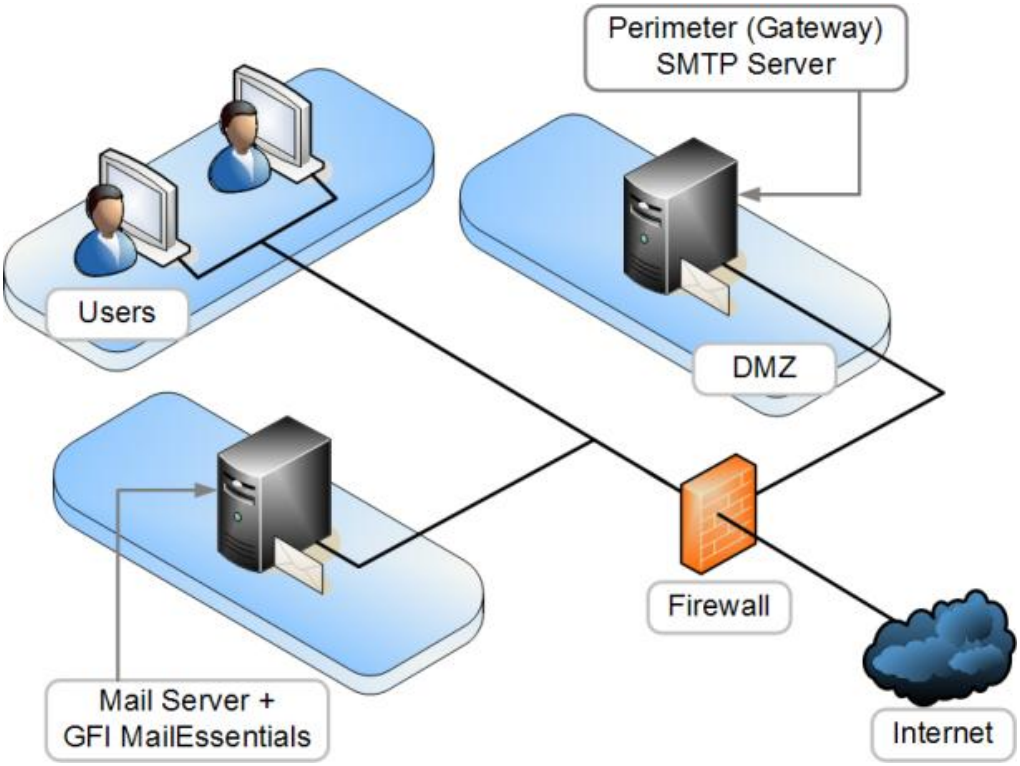


Figure 3 - A typical Perimeter SMTP Relay Server setup

3.5.1 Upgrades from earlier version

If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

Important notes

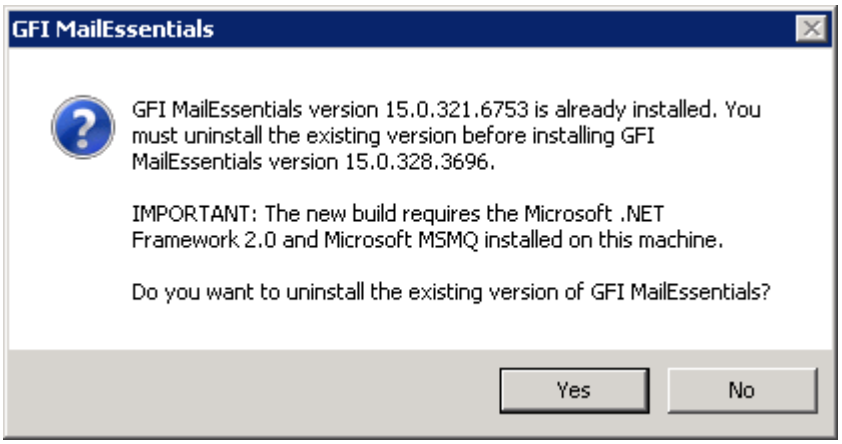
- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.
- On upgrading an existing installation, licensing reverts to trial

version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com.

- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. NO DATA WILL BE LOST.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 9 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to New installations section below.

3.5.2 New installations

Important notes

1. During installation, GFI MailEssentials restarts Microsoft Exchange Server services. This is required to allow GFI MailEssentials components to be registered and started.

2. Before starting installation, close any running Windows applications.

3. When installing GFI MailEssentials on a DMZ, we recommend you use LDAP lookups to get the list of email users (required for user-based configuration/rules e.g. disclaimers) from your SMTP server. The AD of a DMZ usually will NOT include all the network users (email recipients).

Pre-install actions

GFI MailEssentials uses the IIS SMTP service as its SMTP Server and therefore the IIS SMTP service must be configured to act as a mail relay server. This is achieved as follows:

Step 1: Enable IIS SMTP Service

Windows Server 2003

1. Go to **Start ► Control Panel ► Add or Remove Programs ► Add/Remove Windows Components**.
2. Select **Internet Information Services (IIS)** and click **Details**.
3. Select the **SMTP Service** option and click **OK**.
4. Click **Next** to finalize your configuration.

Windows Server 2008

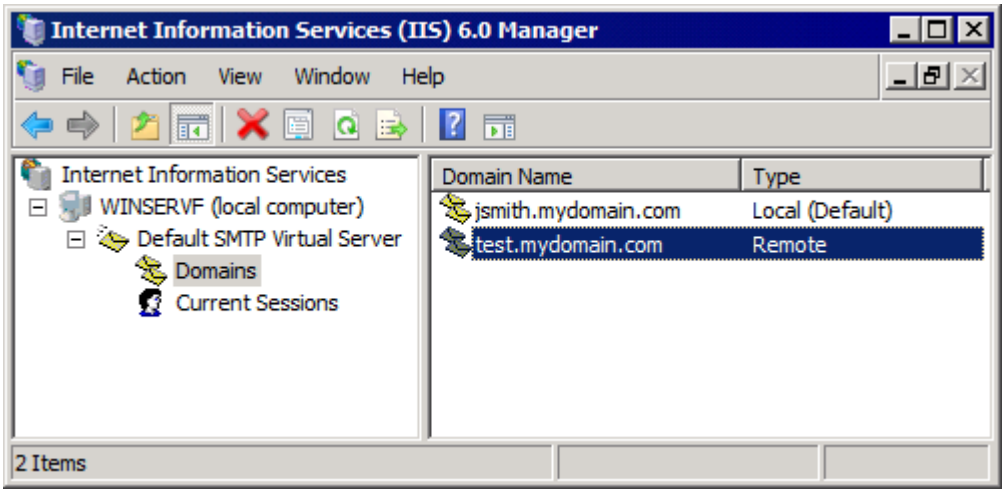
1. Launch the Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server** checkbox.

NOTE: The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize the configuration.

Step 2: Create SMTP domain(s) for email relaying

1. Go to **Start ► Control Panel ► Administrative Tools**.
2. Click on **Internet Information Services (IIS) Manager**.



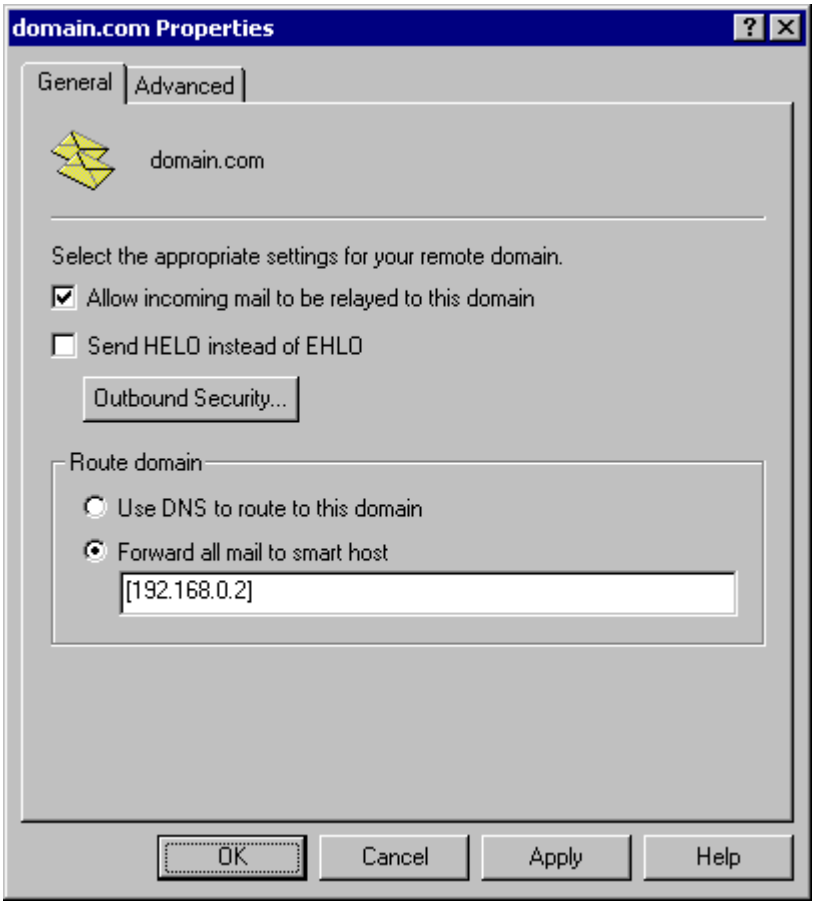
Screenshot 10 - Internet Information Services (IIS) Manager

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.
4. Select the IP address currently assigned to your SMTP server and click **OK**.
5. Expand the **Default SMTP Virtual Server** node.
6. Right click **Domains** and select **New ► Domain**.
7. Select the **Remote** option and click **Next**.
8. Specify domain name (e.g. test.gfi.com) and click **Finish**.

Step 3: Enable email relaying to your Microsoft Exchange server:

1. Right click on the new domain (e.g. test.gfi.com) and select **Properties**.

2. Select the **Allow the Incoming Mail to be Relayed to this Domain** checkbox.



Screenshot 11 - Configure the domain

3. Select the **Forward all mail to smart host** option and specify the IP address of the server managing emails in this domain. IP address must be enclosed in square brackets e.g. [123.123.123.123] so to exclude them from all DNS lookup attempts.

4. Click **OK** to finalize your configuration.

Step 4: Secure your SMTP email-relay server

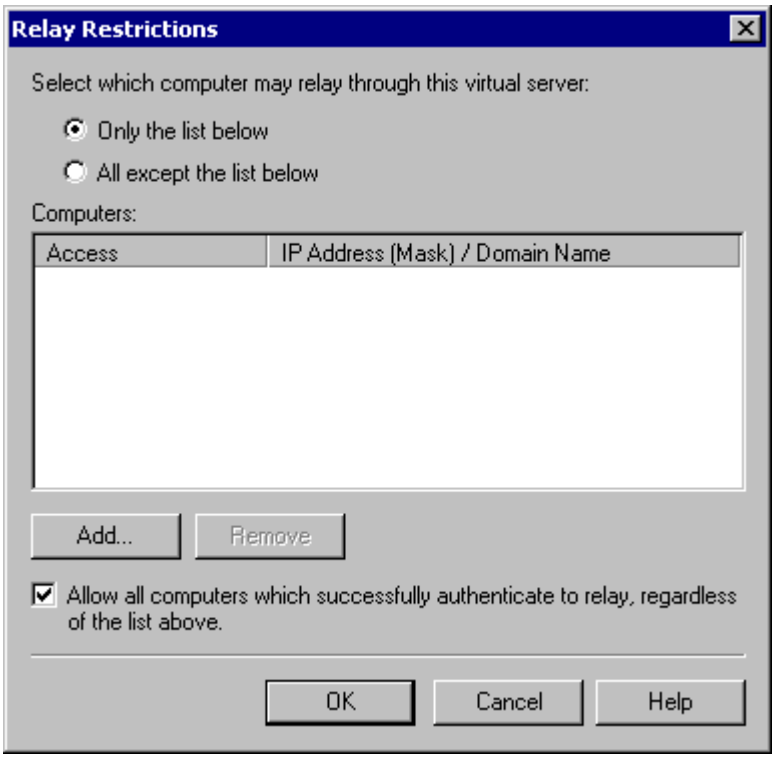
If unsecured, your mail relay server can be exploited and used as an open relay for spam. To avoid this from happening, it is recommended that you specifically define which mail servers can route emails through this mail relay server (i.e. allow only specific servers to use this email relaying setup). To achieve this:

1. Go to **Start ► Control Panel ► Administrative Tools**.

2. Click on **Internet Information Services (IIS) Manager**.

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

4. Click on the **Access** tab and select **Relay**.



Screenshot 12 - Relay options

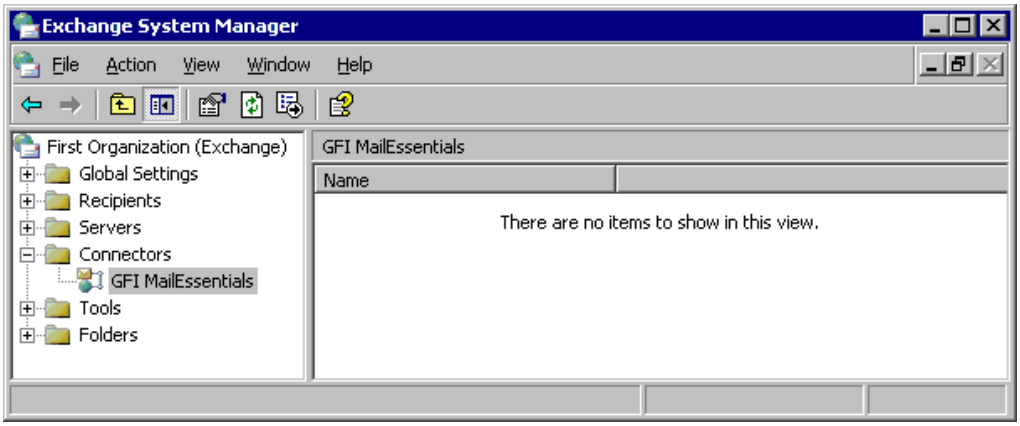
5. Select the **Only the list below** option and click **Add**.

6. Specify IP(s) of the mail server(s) that are allowed to route emails through your mail relay server. You can specify:

- **Single computer -** i.e. Authorize one specific machine to relay email through this server. Use the **DNS Lookup** button to lookup an IP address for a specific host.
- **Group of computers -** i.e. Authorize specific computer(s) to relay emails through this server.
- **Domain -** Allow all computers in a specific domain to relay emails through this server.

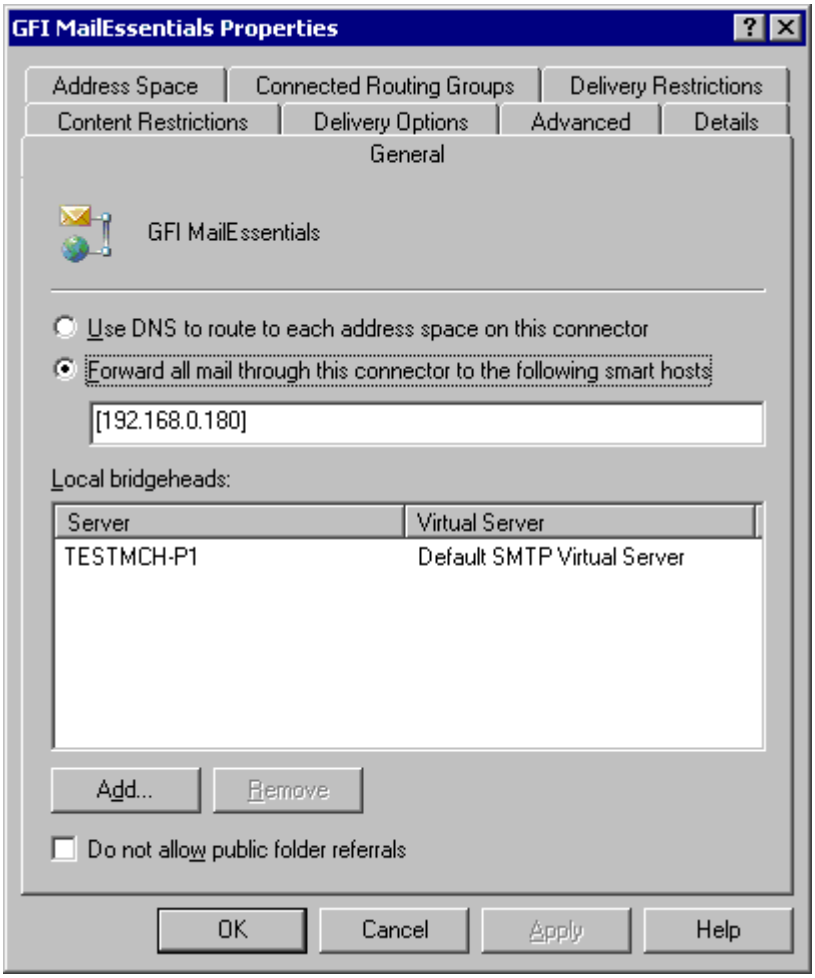
NOTE: The Domain option adds a processing overhead that can degrade SMTP service performance. This is due to the reverse DNS lookup processes triggered on all IP addresses (within that domain) that try to route emails through this relay server.

Step 5: Enable your Microsoft Exchange Server to route emails via mail relay server/GFI MailEssentials



Screenshot 13 - Forwarding email to GFI MailEssentials machine

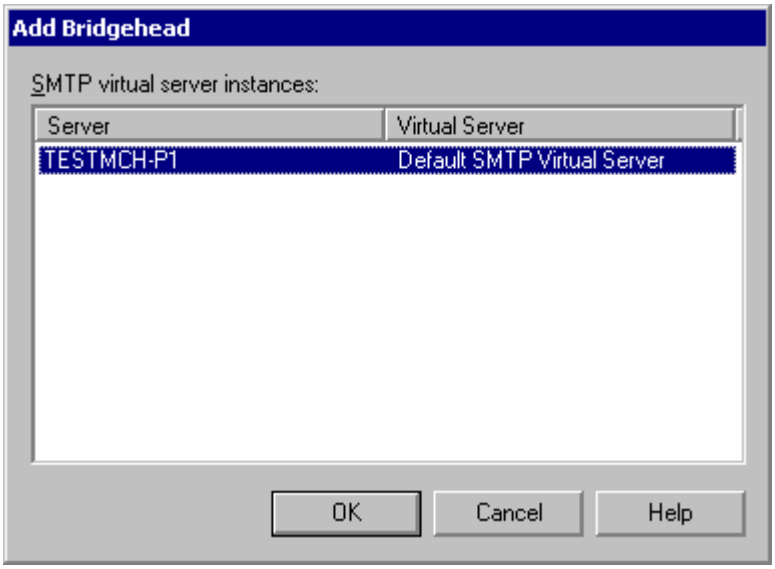
1. Launch Exchange System Manager.
2. Right click **Connectors** node and select **New ► SMTP Connector**.



Screenshot 14 - Specifying IP of GFI MailEssentials machine

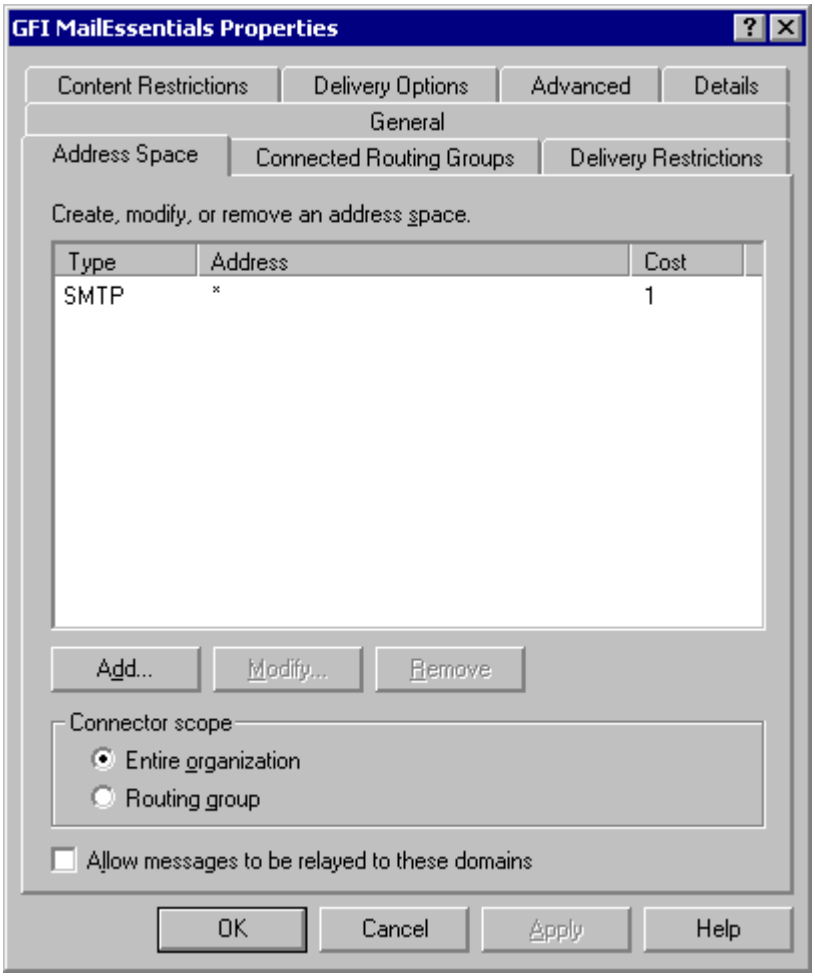
3. Select the **Forward all mail through this connector to the following smart host** option, and specify the IP of your mail relay server within square brackets (i.e. the IP of the machine on which GFI

MailEssentials is installed) e.g. [123.123.1.123].



Screenshot 15 - Adding a bridgehead

4. Click **Add** and select the virtual SMTP Server (i.e. the email relay server on which GFI MailEssentials is running).



Screenshot 16 - Adding SMTP as address space

5. Click on the **Address Space** tab then click **Add**.

6. Select **SMTP** and click **OK**.

7. Click **OK** to finalize your configuration. All emails will now be forwarded to the GFI MailEssentials server.

Step 6: Update your domain MX record to point to mail relay server

Update the MX record of your domain to point to the IP of the new mail relay server. If your DNS server is managed by your ISP, ask your ISP to update the MX record for you.

If MX record is not updated all emails will be routed directly to your email server - hence by-pass GFI MailEssentials anti spam filters.

Verify that MX record has been successfully updated

To verify whether MX record is updated do as follows:

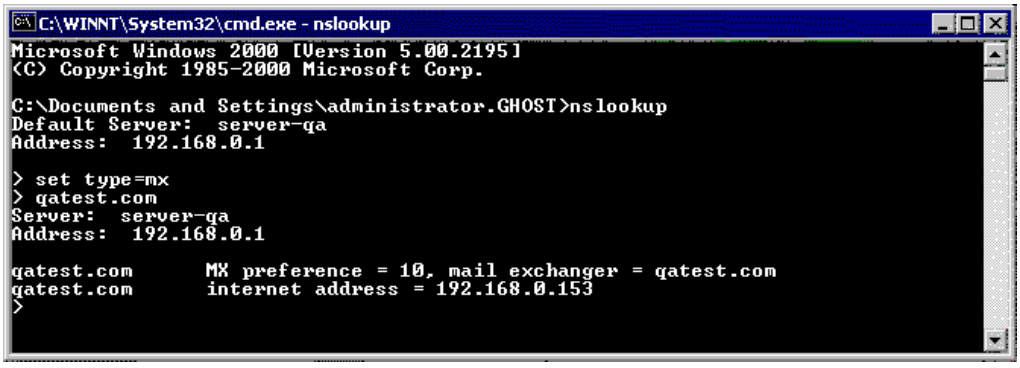
1. Click **Start ► Run** and type: **Command**

2. From the command prompt type in: **nslookup**

3. Type in: **set type=mx**

4. Specify your mail domain name.

The MX record should return the IP addresses of the mail relay servers.



Screenshot 17 - Checking the MX record of your domain

Step 7: Test your new mail relay server

Before proceeding to install GFI MailEssentials, verify that your new mail relay server is working correctly by doing as follows:

Test IIS SMTP inbound connection via test email

1. Send an email from an 'external' account (e.g. Gmail) to an internal email address/user.

2. Ensure that intended recipient received the test email in the respective email client.

Test IIS SMTP outbound connection via test email

1. Send an email from an 'internal' email account to an external account (e.g. Gmail).

2. Ensure that the intended recipient/external user received the test email.

NOTE: You can also use 'Telnet' to manually send the test email and obtained more troubleshooting information. For more information refer

to: http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

Installation procedure

1. Logon to your Microsoft Exchange Server machine using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

3. Select preferred install language and click **Next**.

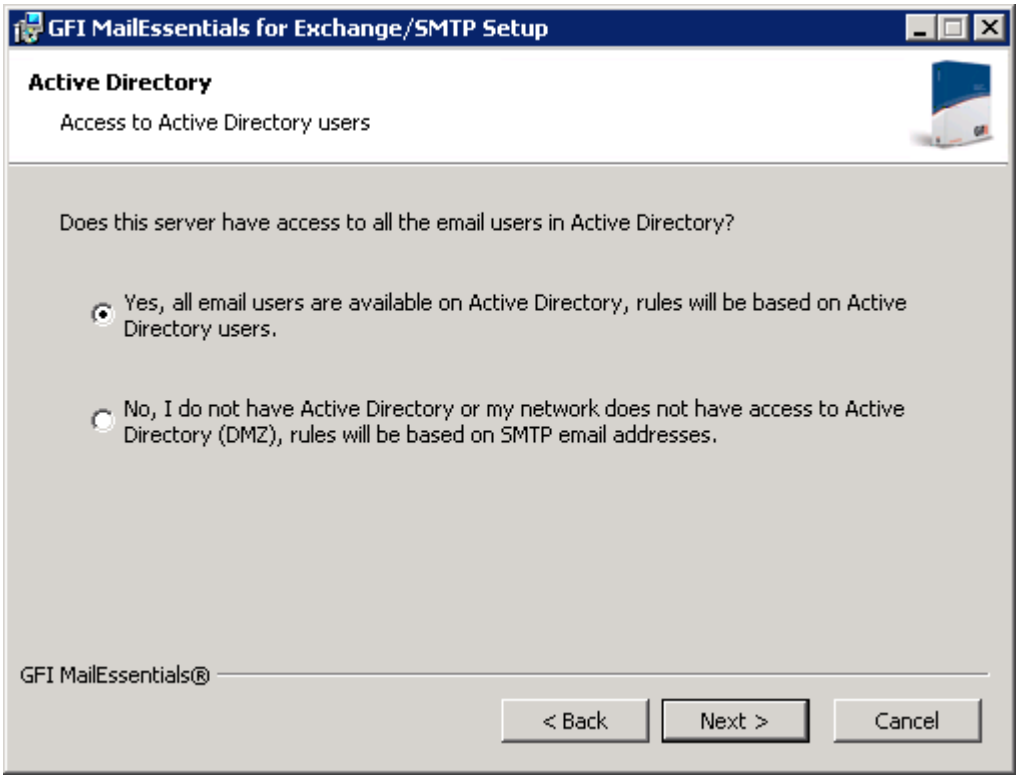
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with this installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

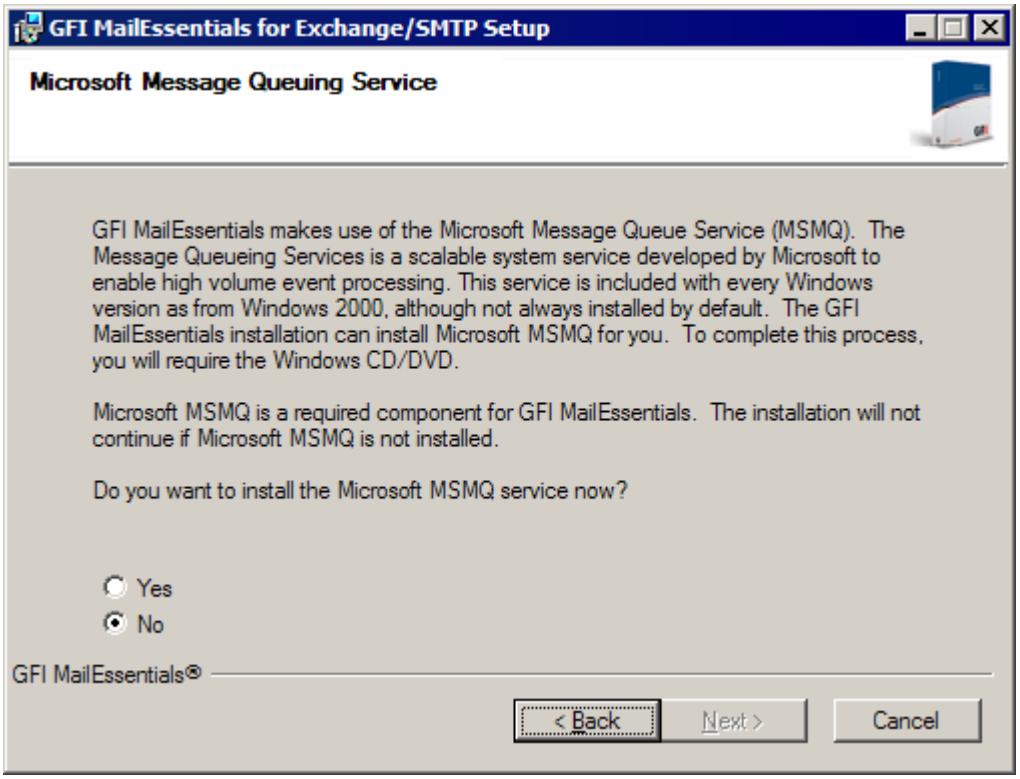
7. Specify user details and enter license key. Click **Next** to continue.

8. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are to be sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 18 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue.


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 19 - Installing Microsoft Message Queuing Service

10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

11. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service.

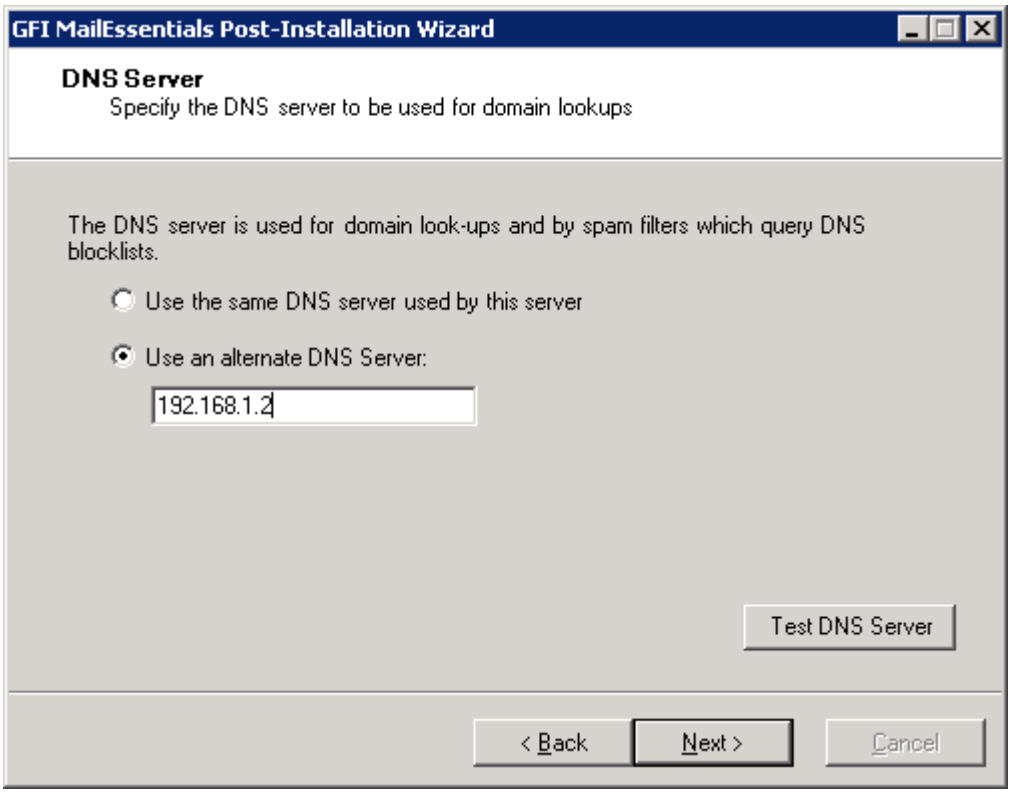
  IMPORTANT: Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.

- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

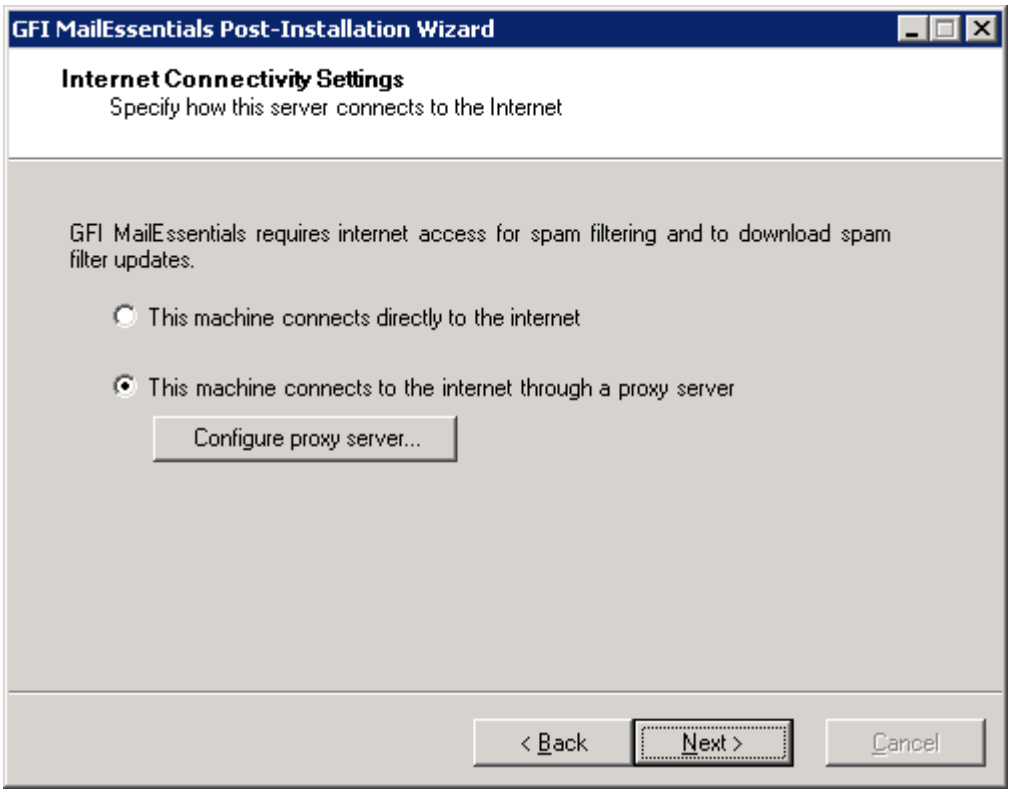

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 20 - DNS Server settings

2. In the **DNS Server** dialog, select:

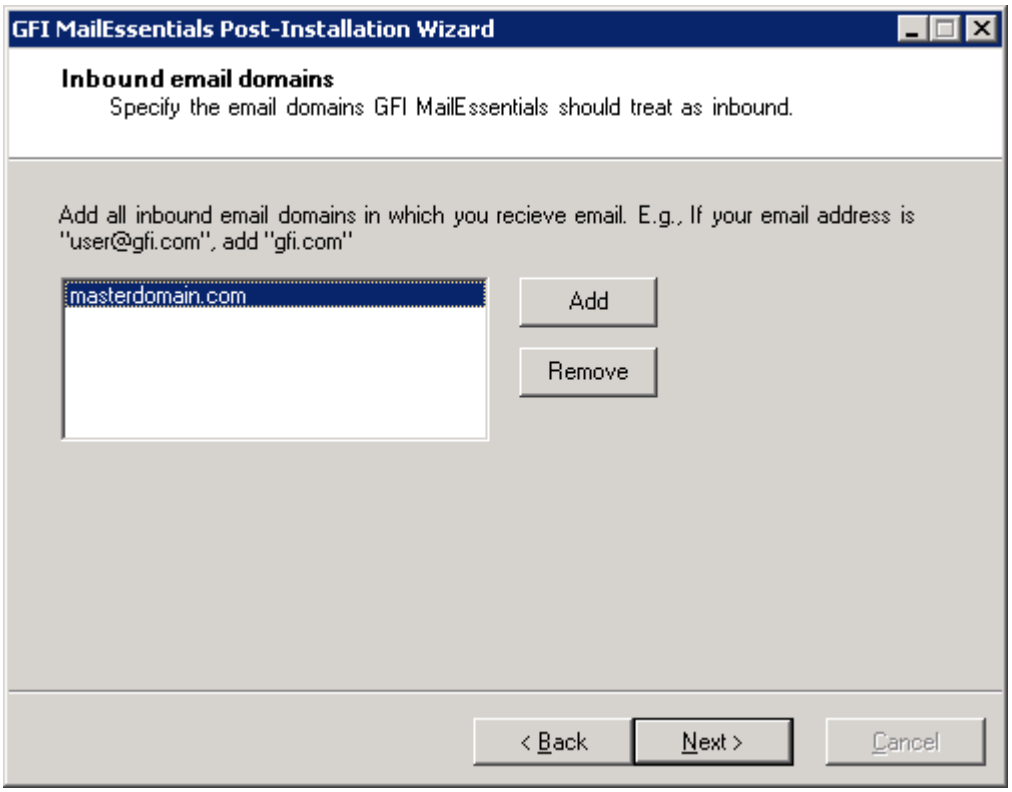
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 21 - Internet connectivity settings

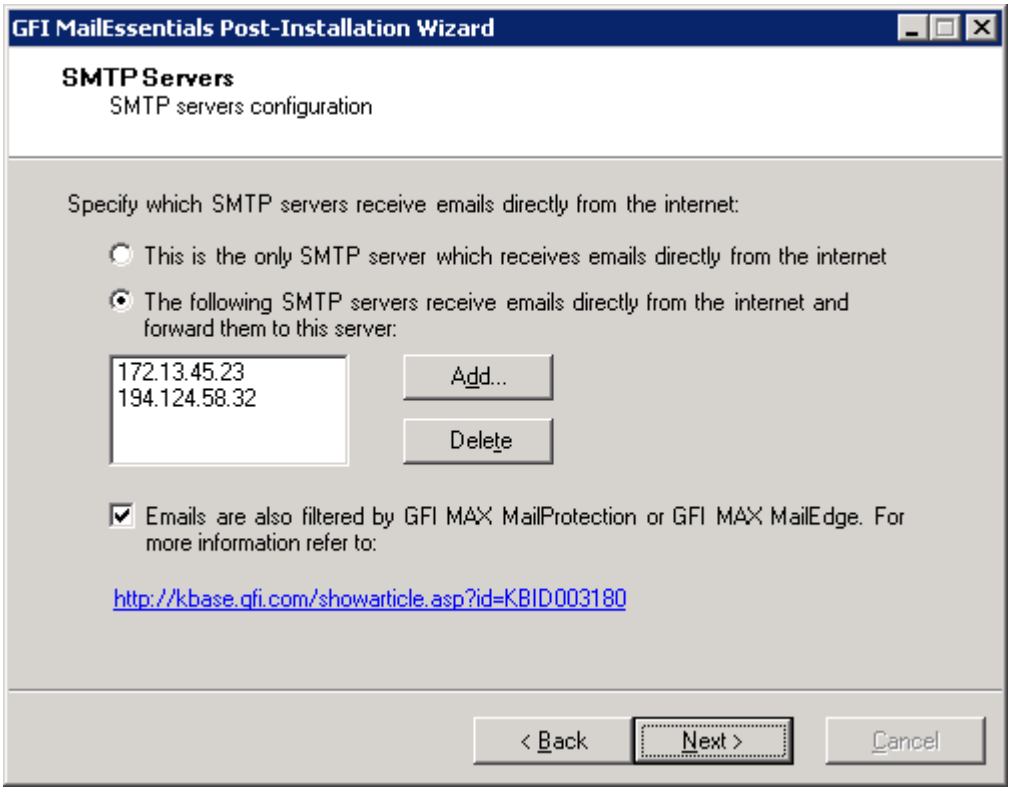
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 22 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 23 - SMTP Server settings

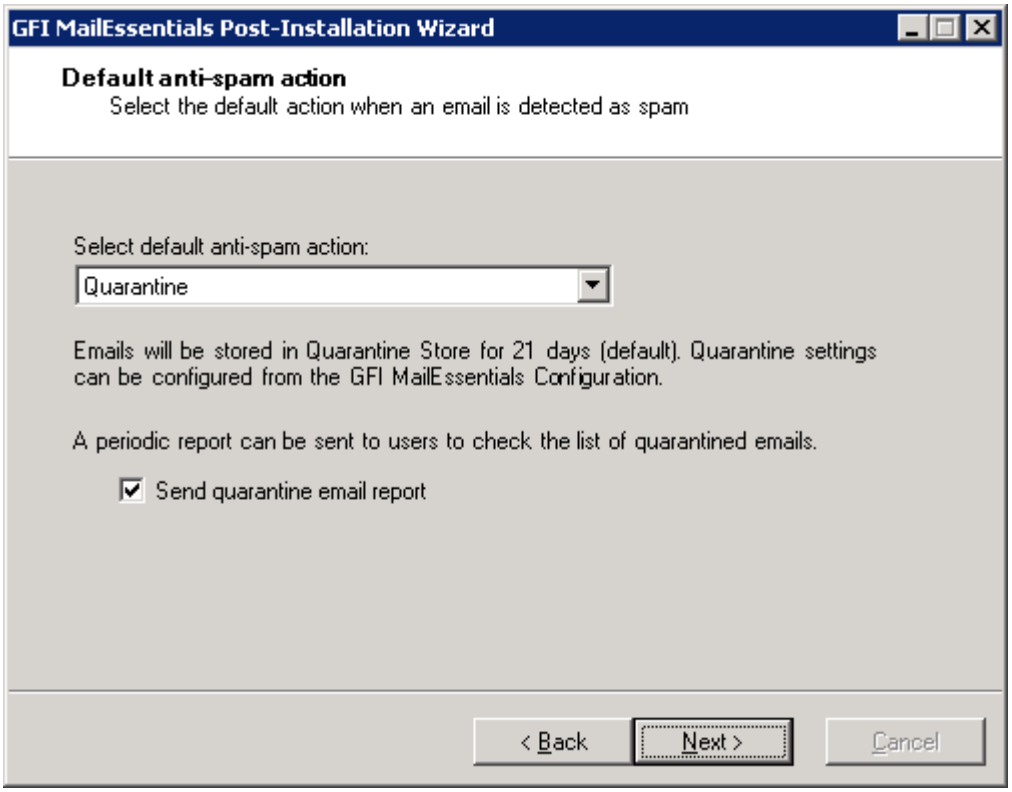
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 24 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

3.6 Installing on Microsoft Exchange 2003 cluster

Introduction

A cluster is a group of servers, technically known as nodes, working collectively as a single server. Such environment provides high availability and fail over mechanisms to ensure constant availability of resources and applications including email infrastructures. If one of the nodes in the cluster fails/is not available, resources and applications switch to another cluster node.

A Microsoft Exchange cluster can be set up in one of 2 modes: active/active or active/passive. GFI MailEssentials supports **ONLY** active/passive clusters. In an active/passive cluster, a 'failover' mechanism ensures that whenever an active cluster fails, one of the available passive nodes becomes active (i.e. takes over the role of the failed node).

In view of the way clusters work, GFI MailEssentials must be installed on all servers/cluster nodes in order to ensure uninterrupted email spam management. GFI MailEssentials installation in a Microsoft Exchange 2003 cluster is a 4-tier process:

- **Process 1:** Install GFI MailEssentials on the Active cluster node.
- **Process 2:** Stop the GFI MailEssentials Legacy Attendant and the GFI POP2Exchange cluster resources and move the Exchange Virtual Server cluster group resource to a passive/other node.
- **Process 3:** Install GFI MailEssentials on another cluster node.
- **Process 4:** Add specific GFI MailEssentials services to the Exchange Virtual Server cluster resource group

Repeat Processes 2, 3 and 4 above for the remaining passive node(s) in the cluster.

3.6.1 Upgrade from earlier version

If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

Pre-upgrade actions

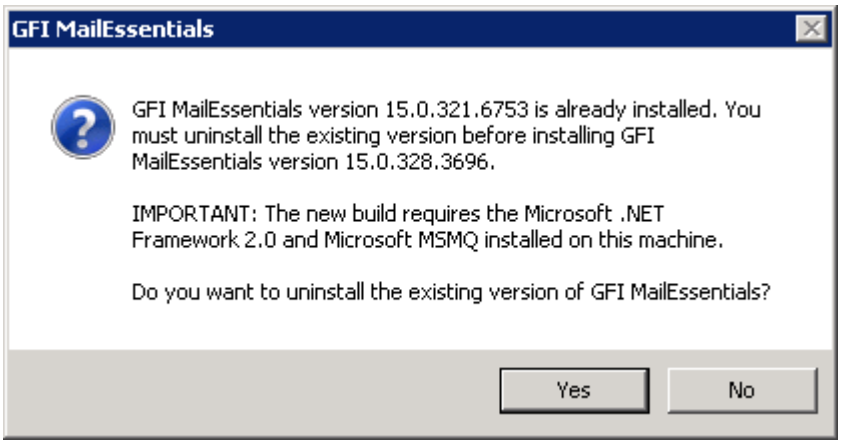
None

Important notes

- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.
- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com
- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. NO DATA WILL BE LOST.
- When upgrading in a Microsoft Exchange cluster environment, all instances of GFI MailEssentials must be upgraded i.e. GFI MailEssentials must be upgraded on all cluster nodes/servers making part of the cluster.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 25 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to the Installation procedure chapter in the section below.

3.6.2 New installations

Important notes

1. Only active/passive cluster setups are supported.

2. Before starting installation, close any running Windows applications.

3. Before starting installation, Microsoft Exchange Server 2003 needs to be installed in clustered mode.

4. Before starting installation ensure that you have a Microsoft Virtual Server cluster group resource with a physical disc cluster available.

Pre-install actions

Create Microsoft Virtual Server cluster group resource

Before you can create an Exchange Virtual Server in a Windows Server cluster, you must first create a cluster resource group. This is the unit of failover in a Windows Server cluster. When Exchange Server is running in a Windows Server cluster, the cluster resource group that contains the Exchange cluster resources is referred to as an Exchange Virtual Server.

To create a resource group for an Exchange Virtual Server in a Windows Server cluster do as follows:

1. Start Cluster Administrator. On prompt, specify cluster details (e.g. name) or click the **browse** button to select cluster in which you want to create an Exchange Virtual Server.

2. In the console tree, right-click **Groups** and select **New ► Group**.

3. In the New Group Wizard that starts automatically, specify a name for the new cluster group, and click **Next**.

4. Click **Finish** to finalize your configuration. This new group object is displayed under Groups in Cluster Administrator.

Installation procedure

Step 1 - Install GFI MailEssentials in the shared hard drive on active server

1. Logon to the active node of your Microsoft Exchange cluster using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

3. Select install language and click **Next**.

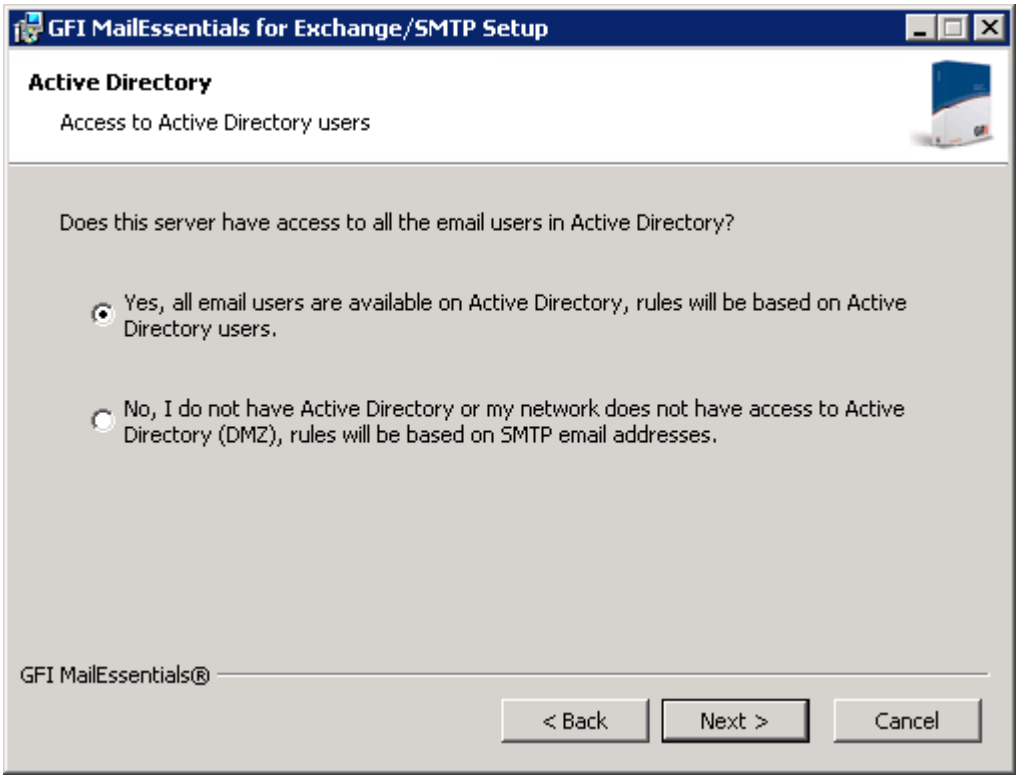
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

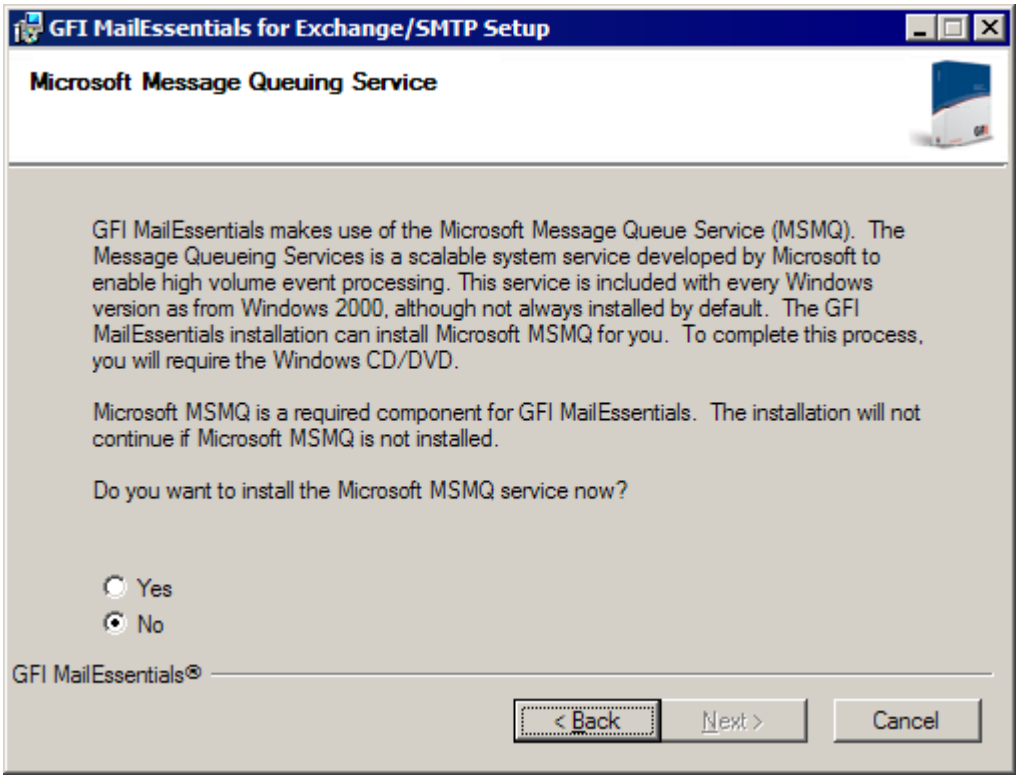
7. Specify user details and enter license key. Click **Next** to continue.

8. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 26 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue**.**


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 27 - Installing Microsoft Message Queuing Service

10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

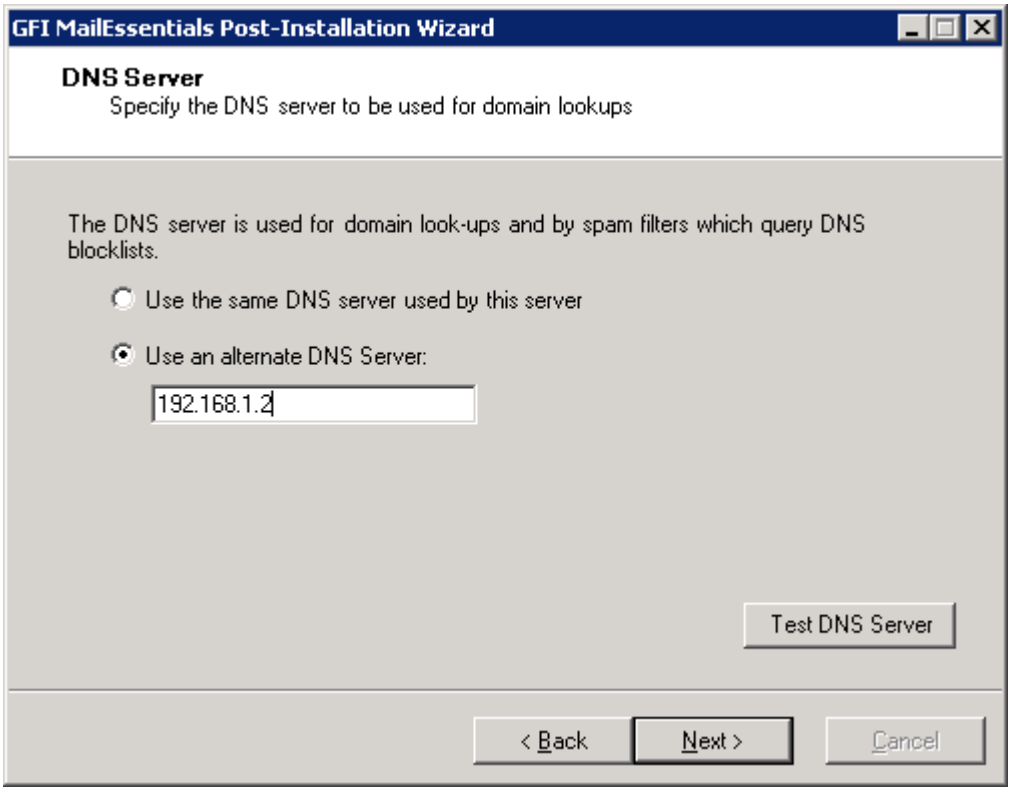
11. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service. Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.
- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

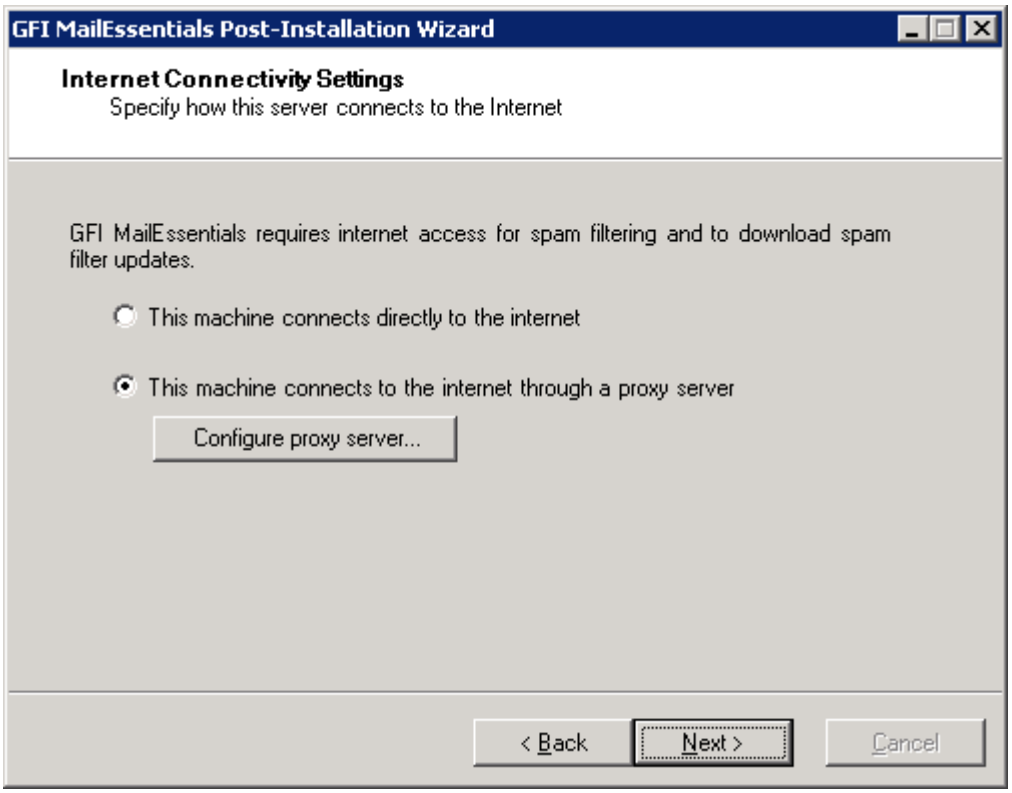

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 28 - DNS Server settings

2. In the **DNS Server** dialog, select:

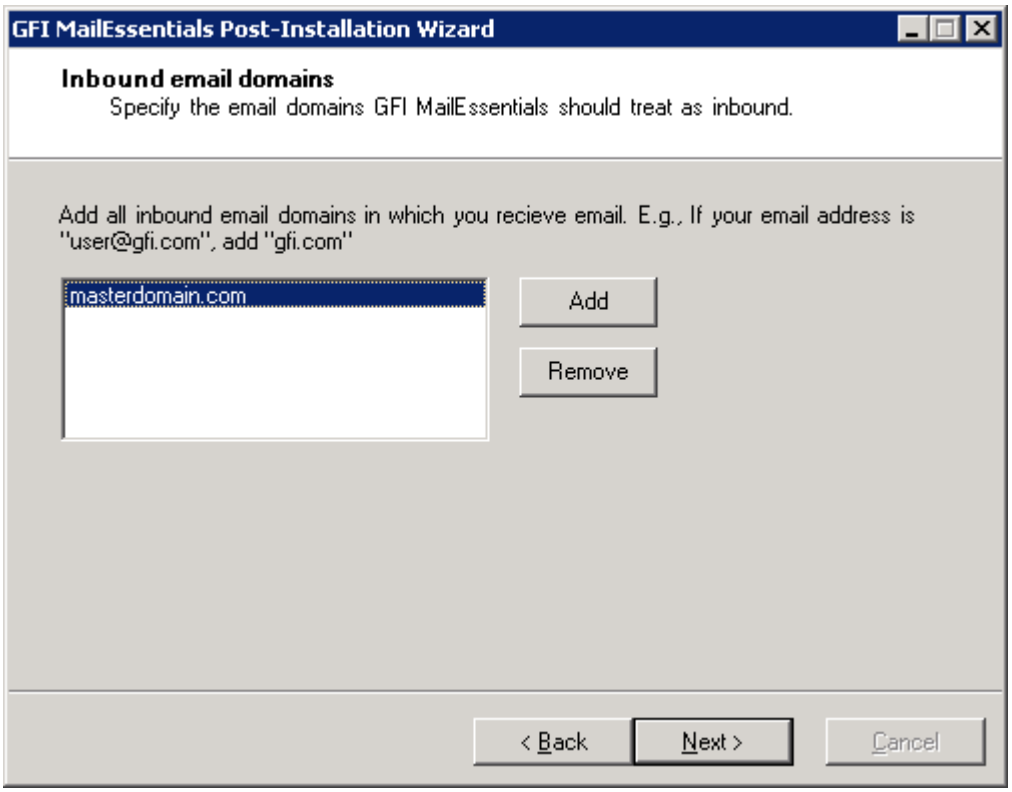
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 29 - Internet connectivity settings

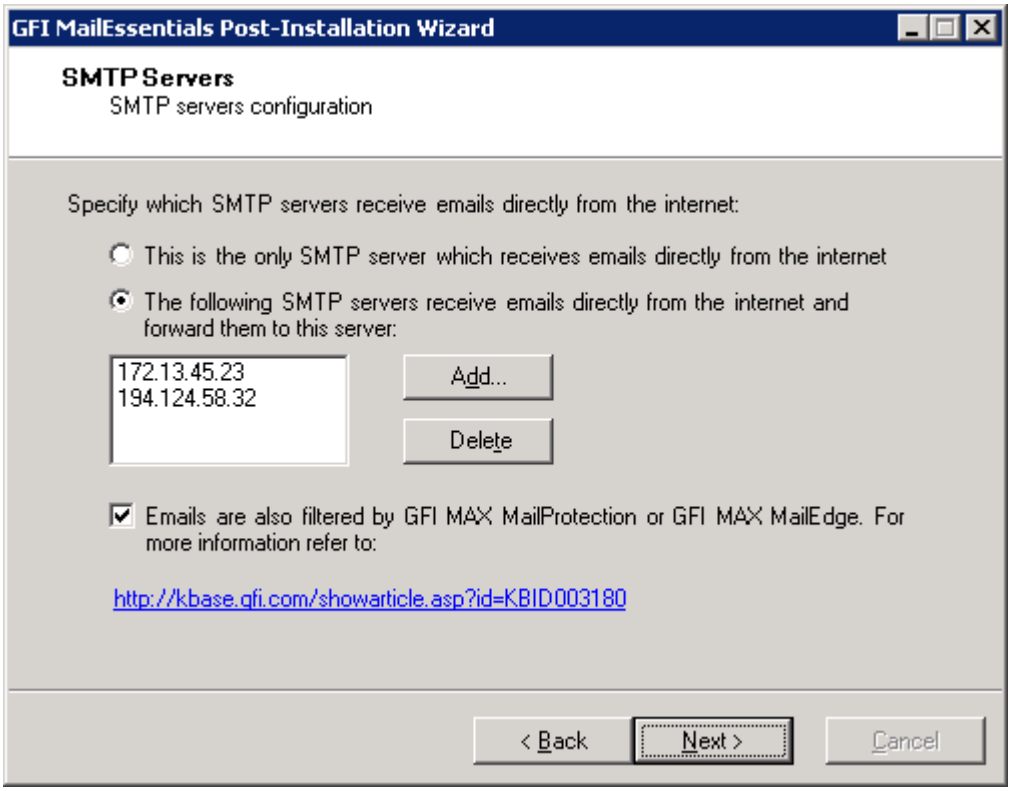
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 30 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 31 - SMTP Server settings

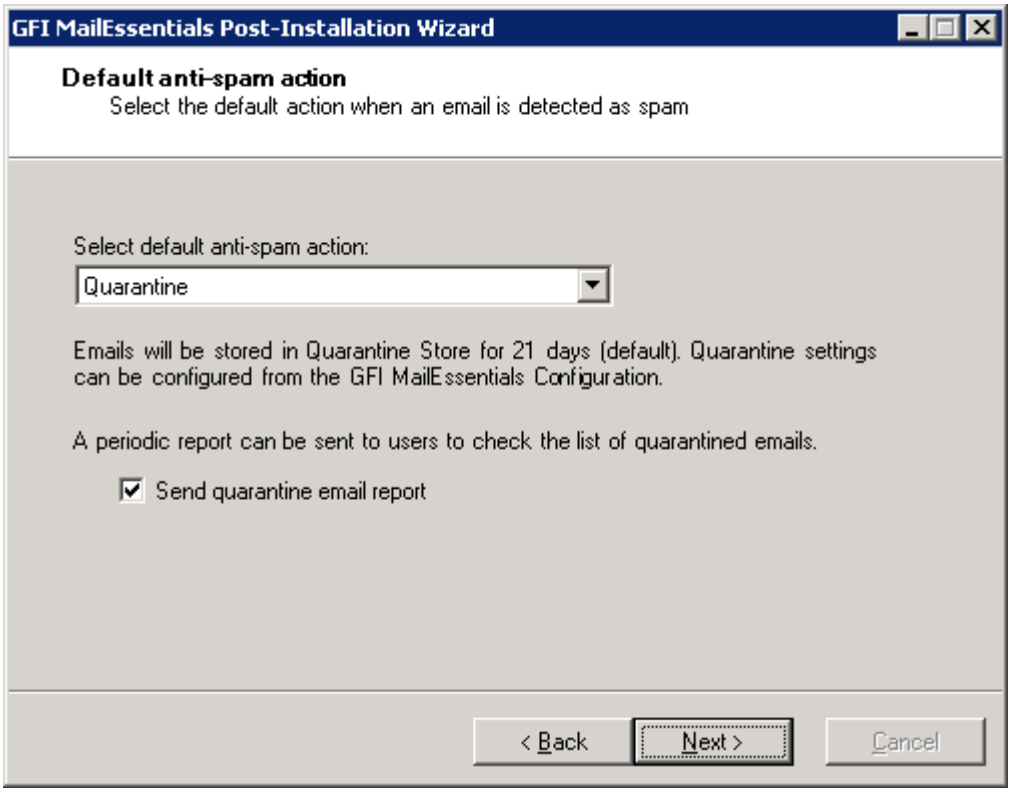
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 32 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

Step 2 - Move the Exchange Virtual Server cluster group

1. Go to **Control Panel ► Administrative Tools ► Cluster Administrator**.

2. Stop the **GFI MailEssentials Legacy Attendant** and the **GFI POP2Exchange** cluster resources.

3. Move the **Exchange Virtual Server** cluster group resource to another node.

Step 3 - Install GFI MailEssentials on a passive server

1. Logon to the passive node of your Microsoft Exchange cluster using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

3. Select install language and click **Next**.

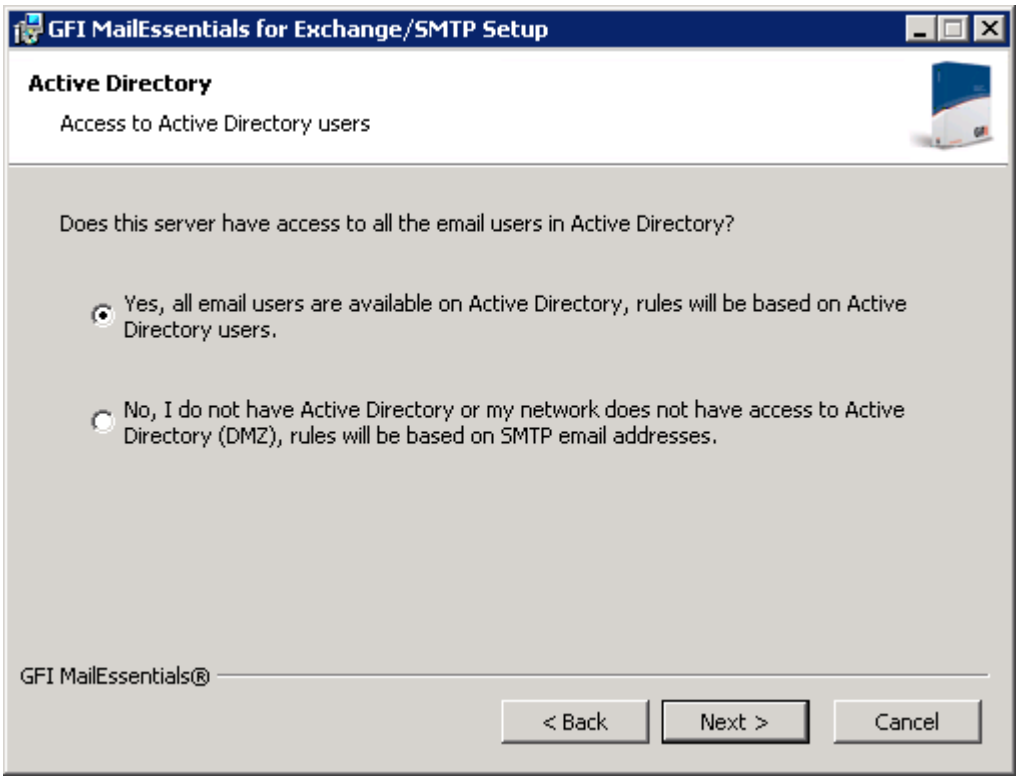
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

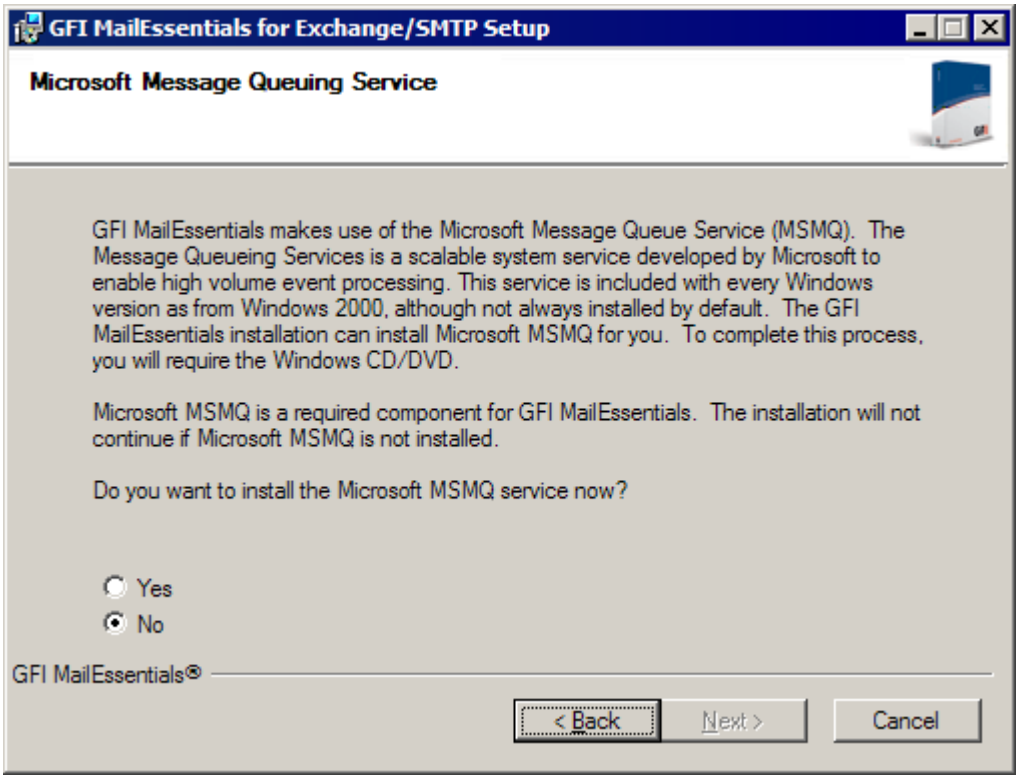
7. Specify user details and enter license key. Click **Next** to continue.

8. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 33 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue**.**


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 34 - Installing Microsoft Message Queuing Service

10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

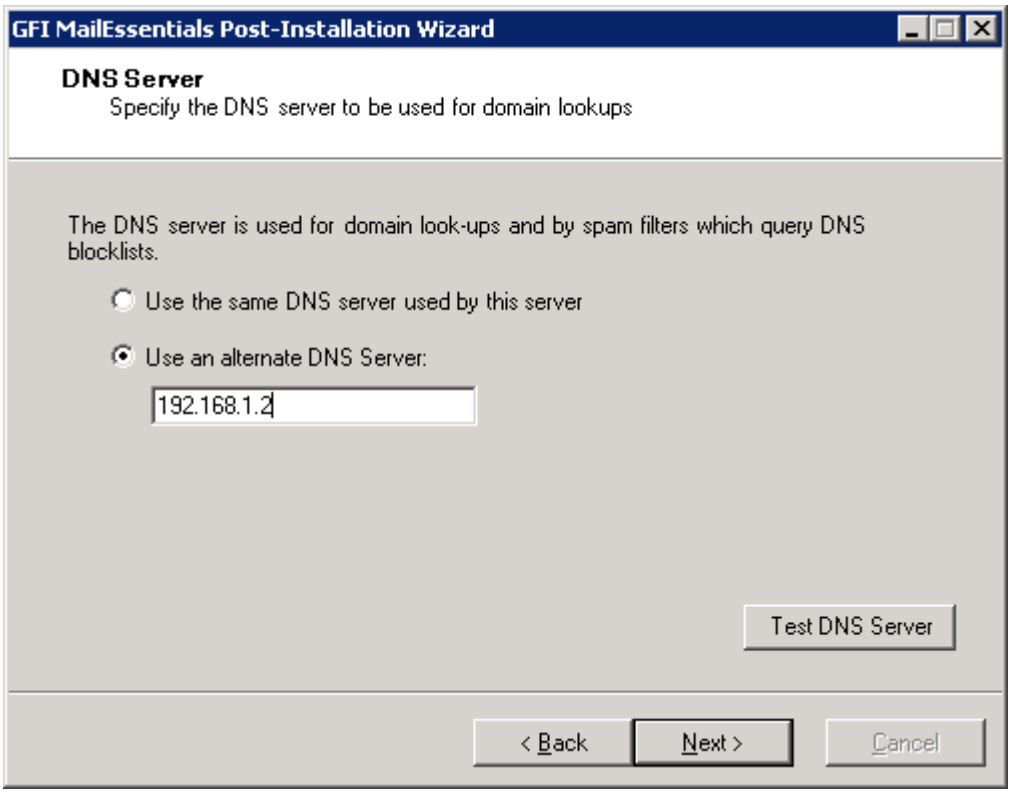
11. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service. Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.
- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

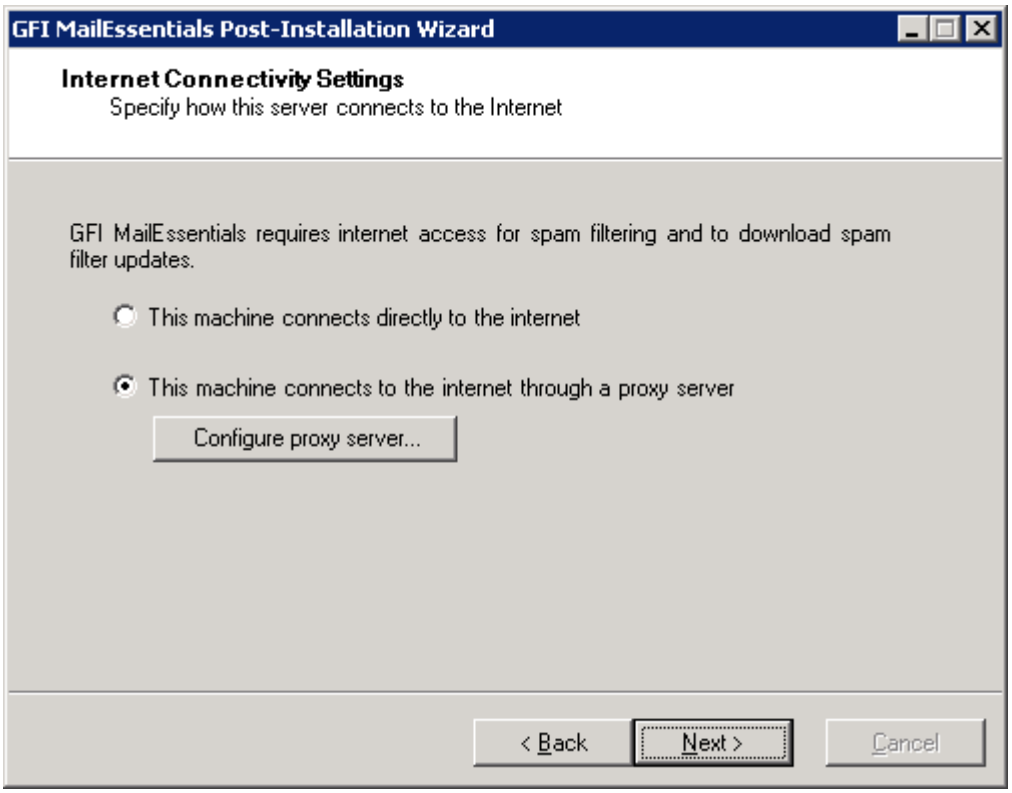

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 35 - DNS Server settings

2. In the **DNS Server** dialog, select:

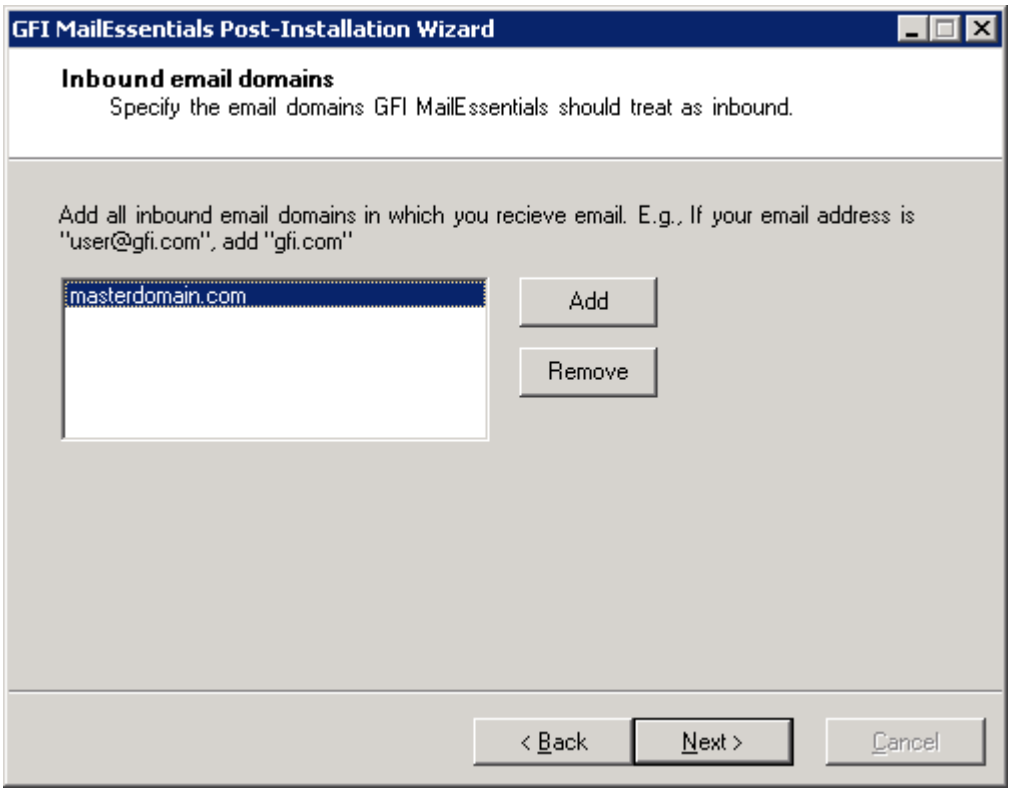
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 36 - Internet connectivity settings

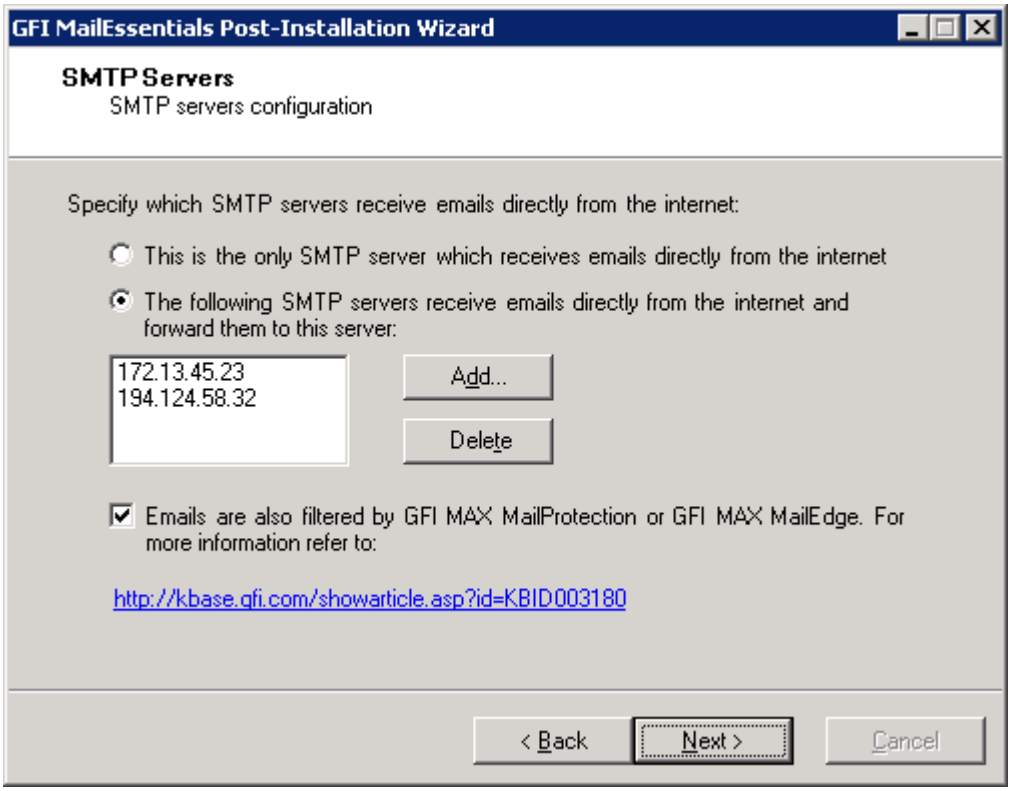
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 37 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 38 - SMTP Server settings

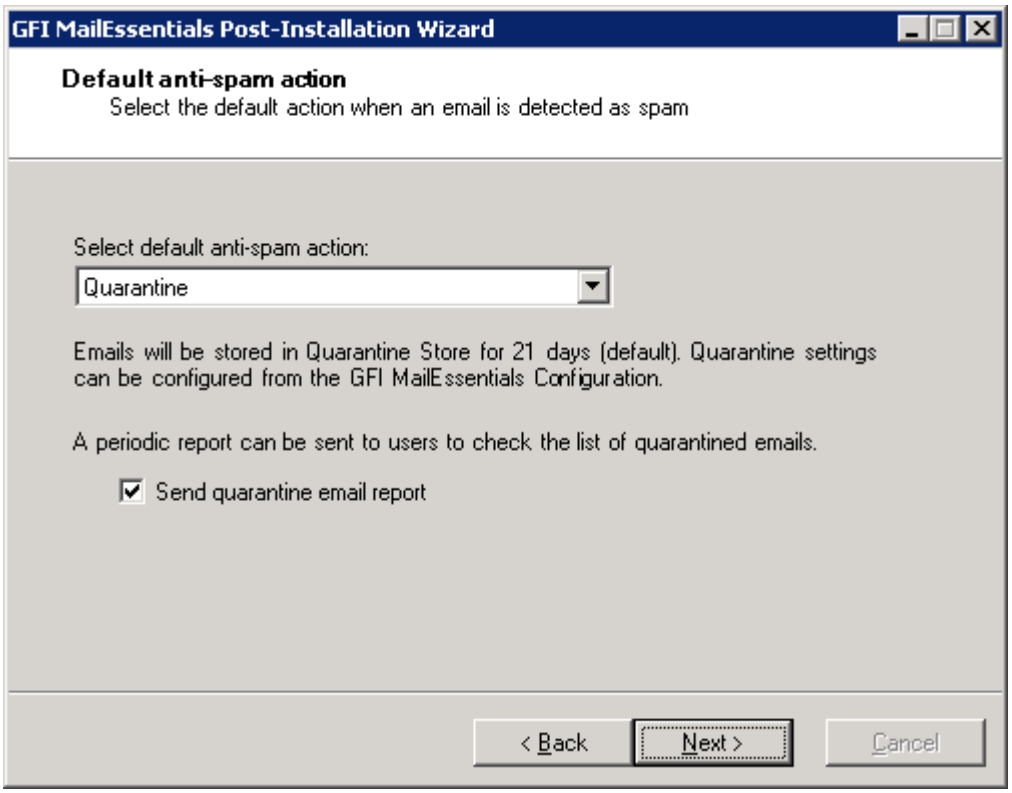
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 39 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

Step 4 - Add specific GFI MailEssentials services to the Exchange Virtual Server cluster resource group

When installing GFI MailEssentials in a clustered windows environment, the product services described below are not automatically included in a cluster resource group. Consequently, if the cluster node on which GFI MailEssentials is running fails, these product services are not moved to another cluster node along with the resource group and they will not be restarted on the new node. As a result, GFI MailEssentials will not start up properly after a failover in a cluster environment.

The services to be added to the Exchange Virtual Server cluster resource group are:

- Service Name: **gfiasmlhost**

  Display name: **GFI MailEssentials Managed Attendant Service**

  Dependencies: **None**

  Start Parameters: **None**

  Registry Replication: **None**
- Service Name: **listserv**

Display Name: **GFI MailEssentials List Server**

Dependencies: **GFI MailEssentials Legacy Attendant**

Start Parameters: **None**

Registry Replication: **None**

- Service Name: **GFIMETRXSVC**

  Display Name: **GFI MailEssentials Enterprise Transfer Service**

  Dependencies: **GFI MailEssentials Legacy Attendant**

  Start Parameters: **None**

  Registry Replication: **None**

To add these services:

1. Go to **Control Panel ► Administrative Tools ► Cluster Administrator**.

2. In the tree view on the left hand side of the 'Cluster Administrator console', expand the cluster root node and then the **Groups** node.

3. Right-click on the **Exchange Virtual Server** cluster group resource to bring up the pop-up menu.

4. Scroll down to the **New** menu item to expand it, and select **Resource** to bring up the New Resource wizard.

5. Enter the service display name in the 'Name' and 'Description' fields. Select 'Generic Service' as Resource Type and select the Exchange Virtual Server cluster group resource as the group to which the new resource will be added. Click **Next**.

6. In the **Possible Owners** dialog, add the nodes of the Exchange cluster to the list of preferred owners. Click **Next**.

7. Select the resource dependencies in the **Dependencies** dialog. Click **Next**.

8. In the 'Generic Service Parameters' dialog, enter the service name, and leave the start parameters text box empty. Click **Next**.

9. Click **Finish** to finalize your configuration. Do not add any keys in the 'Registry Replication' dialog.

10. Repeat from step 3 to 8 above for each service mentioned above.

11. Right-click on the newly added resource(s) and select **Bring Online** to enable services. These resources are visible in the list of cluster resources of the Exchange Virtual Server cluster.

4 Installation for Microsoft Exchange 2007 & 2010

4.1 Introduction

GFI MailEssentials installation depends on your network infrastructure, i.e. Microsoft Exchange 2007/2010 or SBS 2008/2011 setup. You can install this product on:

- **Same server running Microsoft Exchange or SBS:** This setup is typically used to filter email spam on Microsoft Exchange or SBS servers set to receive emails directly from 'outside' (i.e. the internet).
- **Mail gateway or relay/perimeter server:** This type of installation is commonly used to filter spam in distributed email infrastructures - especially those running a DMZ. In this environment a dedicated machine is set to relay emails to another server running Microsoft Exchange. Here, GFI MailEssentials is typically installed on the mail relay server so that email spam is filtered before reaching your Microsoft Exchange server. This setup reduces network traffic, email storage and processing requirements on your email infrastructure.
- **Microsoft Exchange Server 2007/2010 clusters:** This type of installation is commonly used to filter spam within environments where clusters are used as disaster prevention and recovery mechanisms.

4.2 System requirements

4.2.1 Software

Supported operating systems

- Microsoft Windows Server 2008 x64
- Microsoft Windows Server 2008 x86 (Installations on gateway/perimeter server only)
- Microsoft Small Business Server (SBS) 2008/2011 Standard

Mail Servers

- Microsoft Exchange Server 2010
- Microsoft Exchange Server 2007

Other components

- Microsoft .NET Framework 2.0
- Microsoft XML core services: This is required by the GFI MailEssentials reporter to enable anti spam report generation. For UK/US English OS this is installed automatically by GFI MailEssentials. For other languages, this can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- Microsoft Message Queuing Services.
- Microsoft Exchange Server MAPI Client and Collaboration Data Objects 1.2.1. This can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en
- Internet Information Services (IIS) 6 or 7 WWW service, when using Quarantine or Archive Web Interface.

4.2.2 Hardware

Processor

- **Minimum:** Intel Pentium or compatible 1 GHz 32-bit processor
- **Recommended:** x64 architecture-based server with Intel 64 architecture or AMD64 platform

Memory

- **Minimum:** 1GB RAM
- **Recommended:** 2GB RAM

Physical Storage

- **Minimum:** 500MB for installation, 2GB for execution
- **Recommended:** 500MB for installation, 4GB for execution

4.3 Important settings

4.3.1 Antivirus and backup software

Antivirus and backup software may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials

Disable third party antivirus and backup software from scanning the following folders:

x86 installations (32-bit)	x64 installations (64-bit)
<..\Program Files\GFI\MailEssentials>	<..\Program Files (x86)\GFI\MailEssentials>
<..\Program Files\Common Files\GFI>	<..\Program Files (x86)\Common Files\GFI>
<..\Inetpub\mailroot> If installed on a gateway machine.	

<..*Program Files**Exchsrvr**Mailroot*> If installed on the same machine as Microsoft Exchange 2007/2010.

4.3.2 Firewall port settings

Configure your firewall to allow the following port connections. These ports are used by GFI MailEssentials to connect to GFI servers:

- **DNS (Port 53)** - Used by anti spam filters (IP DNS Blocklist, Sender Policy Framework, Header Checking).
- **FTP (Ports 20 and 21)** - Used by GFI MailEssentials to connect to 'ftp.gfisoftware.com' and retrieve latest product version information.
- **HTTP (Port 80) -** Used by GFI MailEssentials to download product patch and anti spam filter updates (i.e. SpamRazer, Anti-Phishing, and Bayesian anti spam filters) from the following locations:
  - 'http://update.gfi.com'
  - 'http://update.gfisoftware.com'
  - 'http://support.gfi.com
  - 'http://db11.spamcatcher.net' (GFI MailEssentials 14 or earlier)
  - 'http://sn92.mailshell.net' (GFI MailEssentials 14 SR1 or later)
- **Remoting (Ports 8021)** - Used in the latest builds of GFI MailEssentials for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server.

  NOTE: Ensure that no other applications (except GFI MailEssentials) are listening on port 8021.
- **(OPTIONAL) LDAP (Port 389)** - Used by GFI MailEssentials to get email addresses from SMTP server. ONLY required if the server running GFI MailEssentials does not have access/cannot get list of users from Active Directory e.g. in a DMZ environment or other environment which does not use Active Directory.

4.4 Installing on Microsoft Exchange or SBS server

4.4.1 Upgrade from earlier version

If you are currently using a previous version of GFI MailEssentials (version 12 or 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

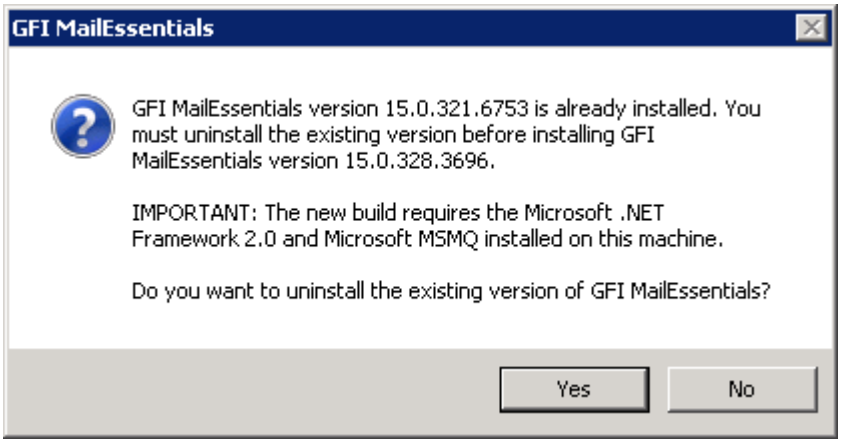
Important notes

- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.
- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com

- You cannot change the installation path during GFI MailEssentials upgrades.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 40 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to New installations section below.

4.4.2 New installations

Important notes

1. During installation, GFI MailEssentials restarts Microsoft Exchange Server services. This is required to allow GFI MailEssentials components to be registered and started.

2. Before starting installation, close any running Windows applications.

3. Since Microsoft Exchange Server 2007/2010 can only be installed on Windows Server 2008 64-bit, GFI MailEssentials 64-bit version is required.

Installation procedure

1. Logon to your Microsoft Exchange Server machine using administrator credentials.

2. Double click **mailessentials2010_x64.exe**.

3. Select install language and click **Next**.

4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

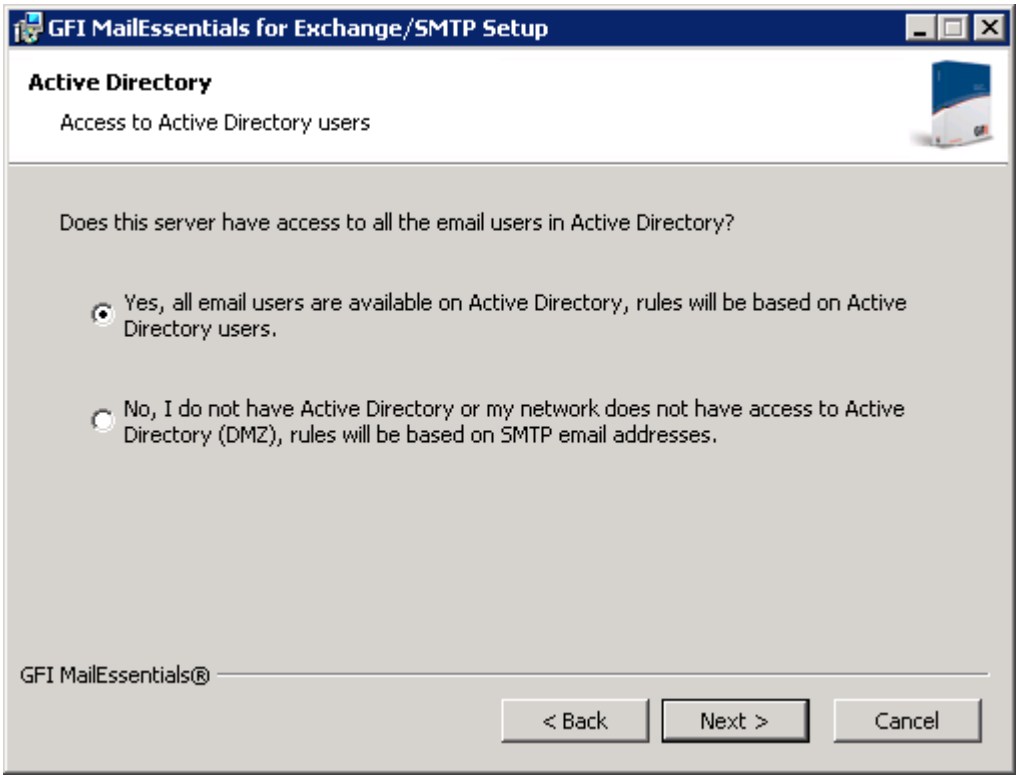
5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

7. Specify user details and enter license key. Click **Next** to continue.

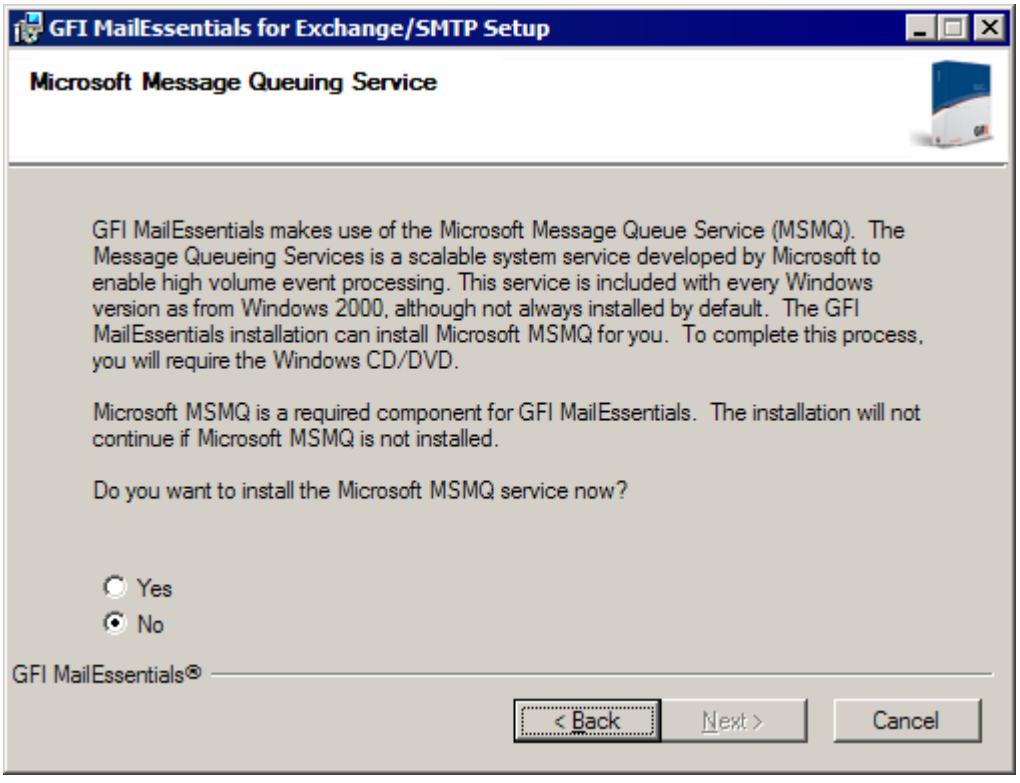
8. Specify the email address where notifications (e.g. failed anti spam

filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 41 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue**.**


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 42 - Installing Microsoft Message Queuing Service

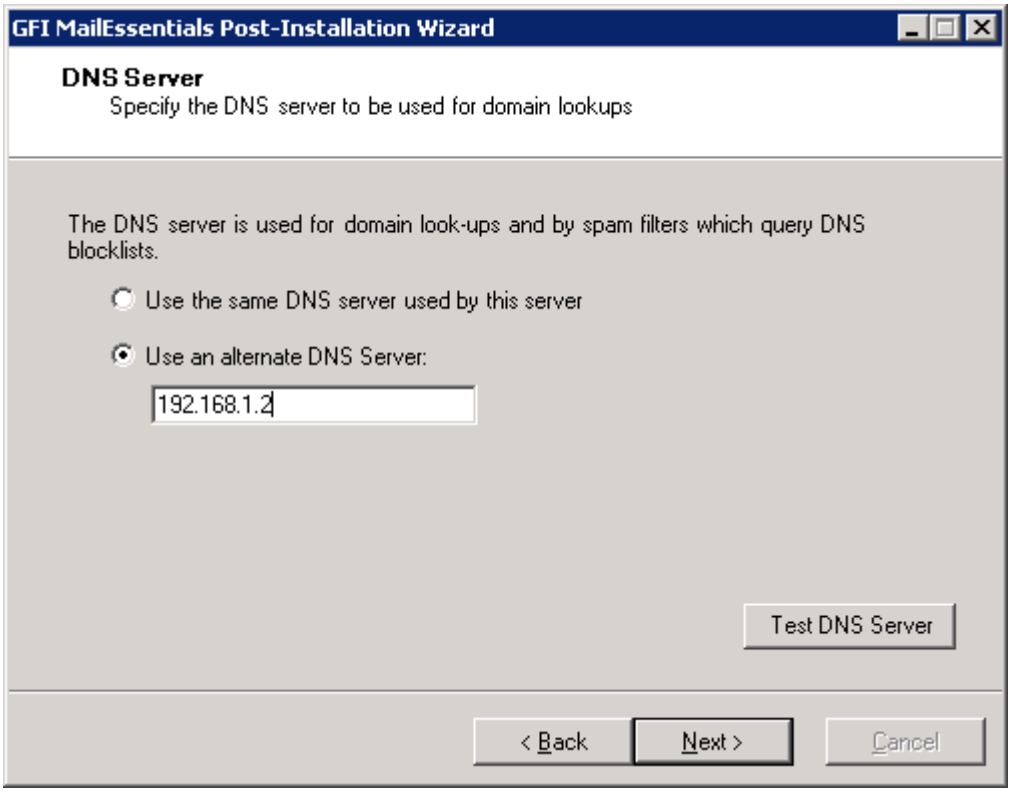
10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

11. Click **Finish** to finalize your installation. On completion, setup will:

- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from: http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

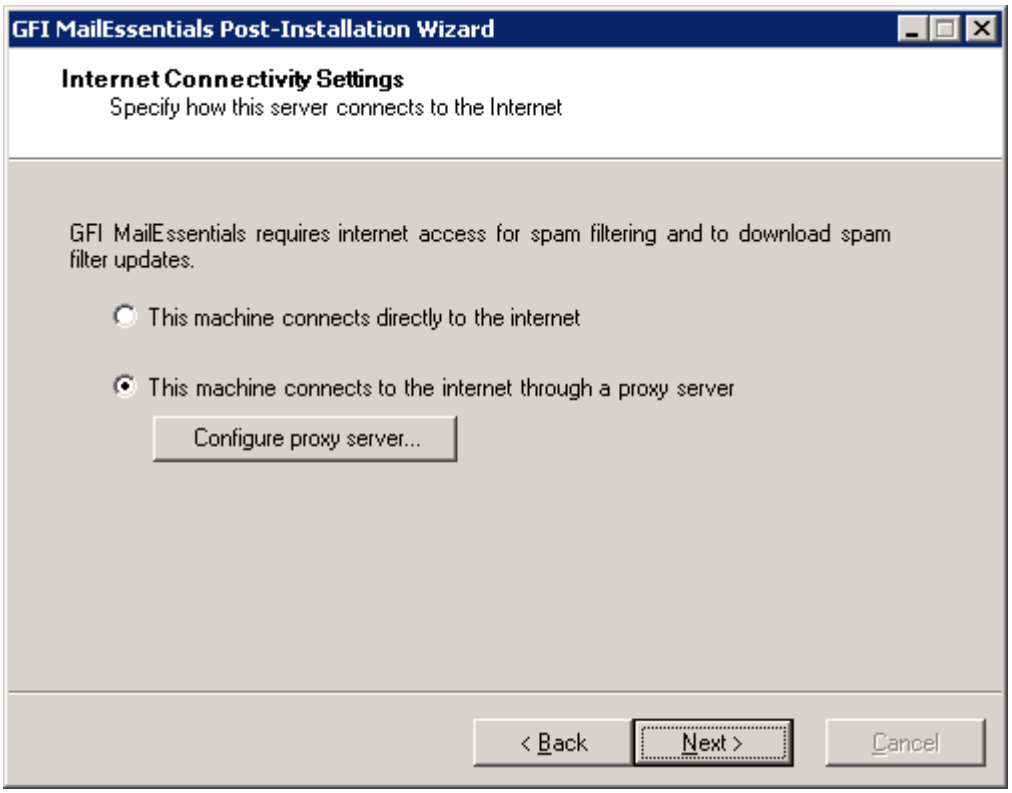

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 43 - DNS Server settings

2. In the **DNS Server** dialog, select:

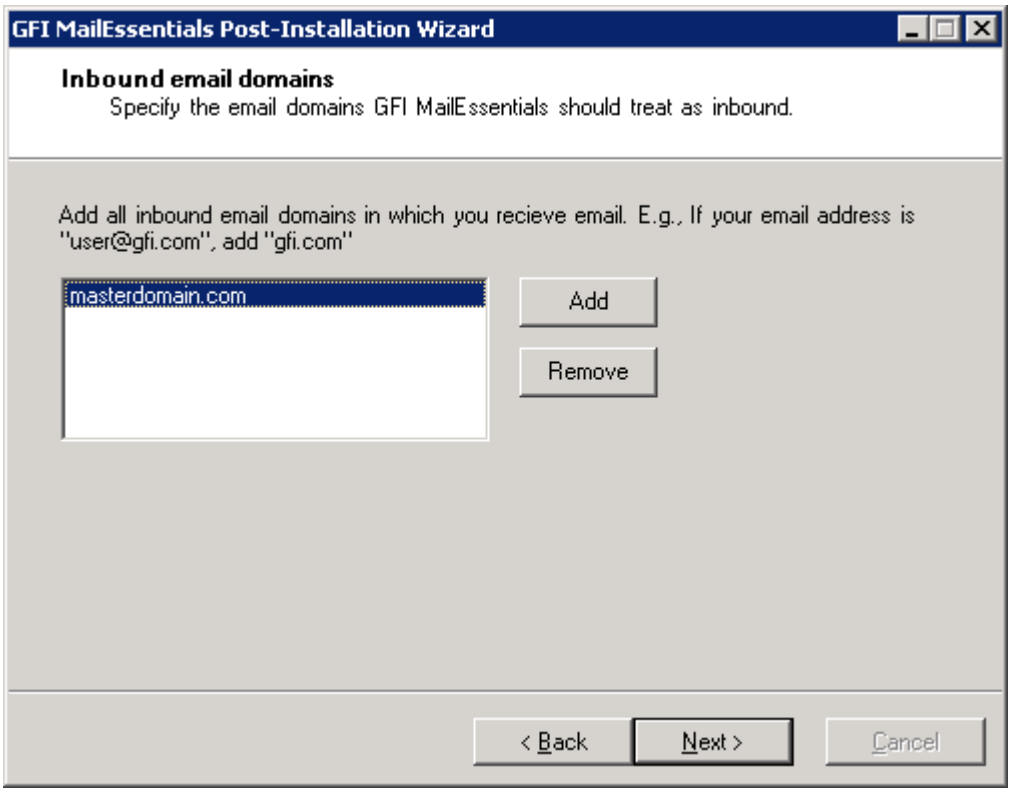
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 44 - Internet connectivity settings

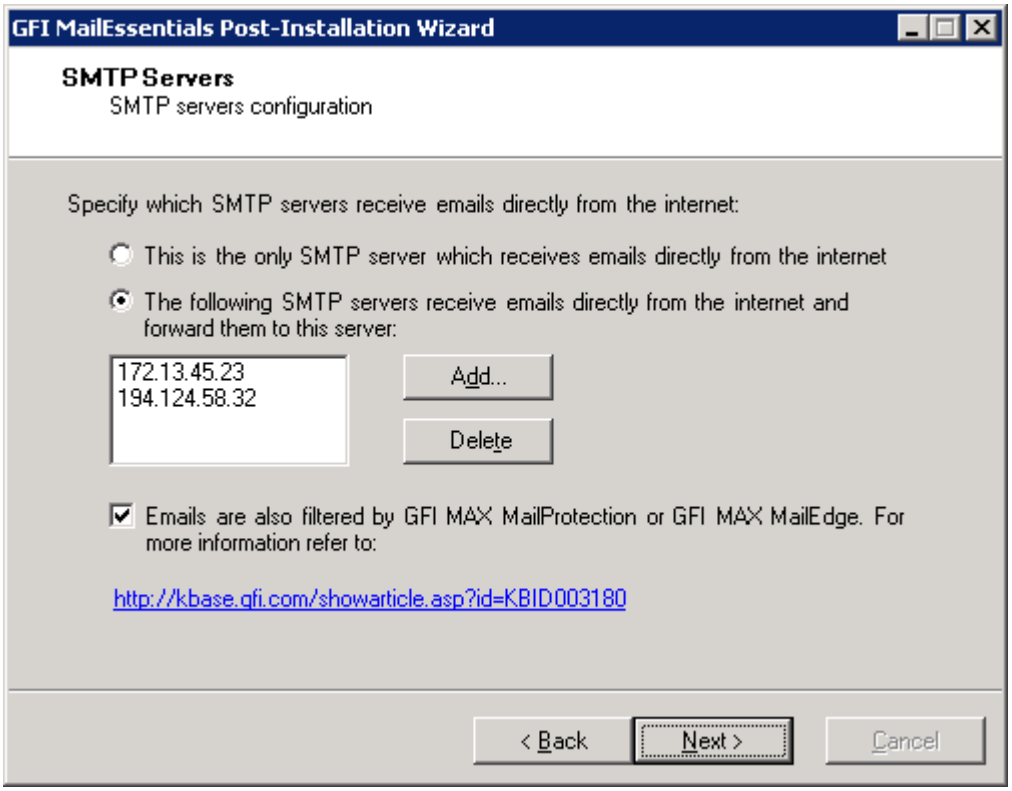
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 45 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 46 - SMTP Server settings

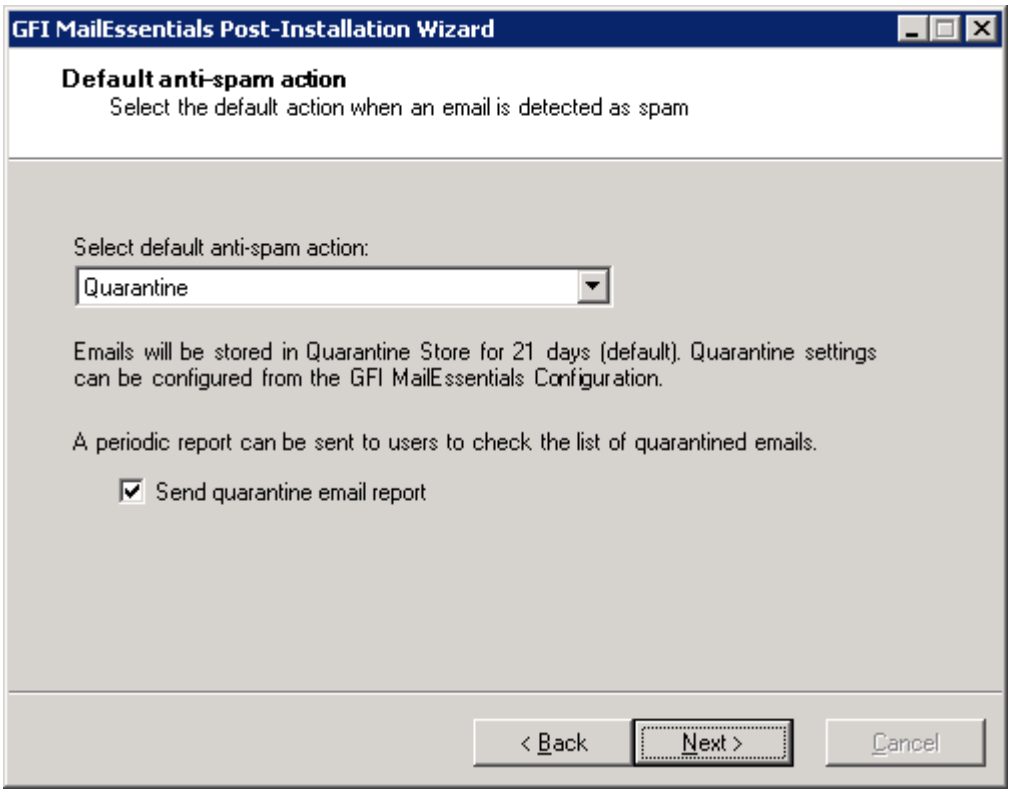
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.

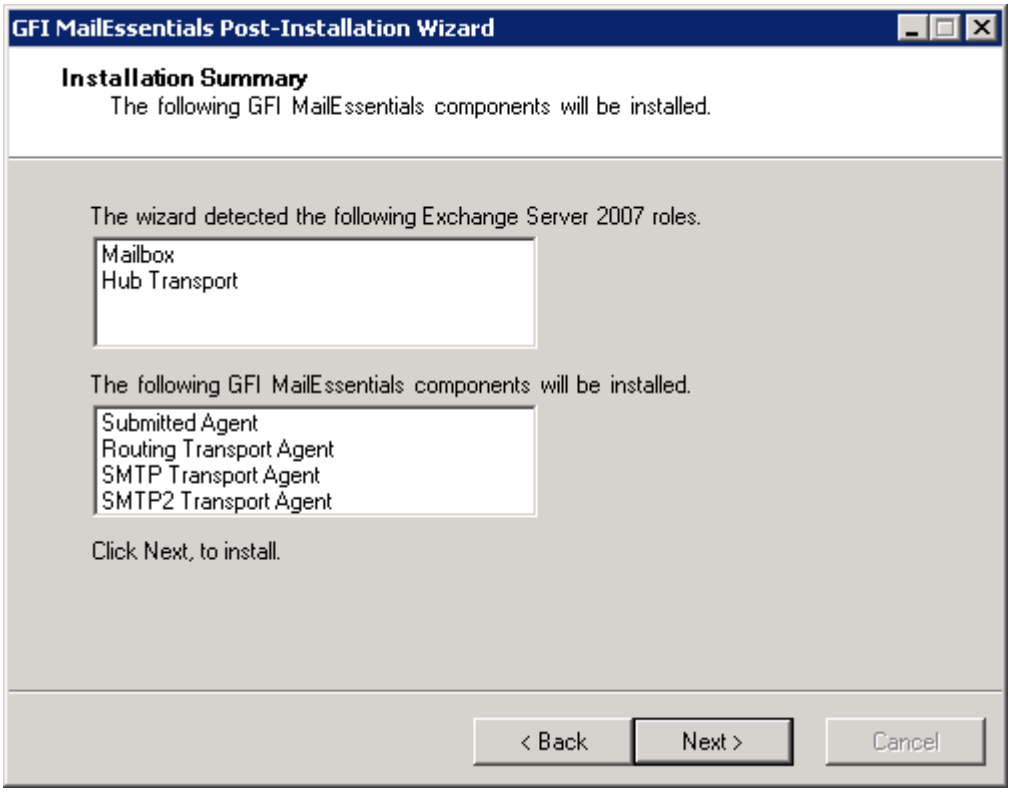

GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 47 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

NOTE: When installing on Microsoft Exchange 2010 and the default action selected is **Move to mailbox sub-folder**, a user with impersonation rights must be created. Select whether to let GFI MailEssentials automatically create the user or manually specify the credentials and click **Set impersonation rights** to assign the required rights to the specified user. This user must be dedicated to this feature only and the credentials must not be changed, otherwise the Move to Exchange folder feature will not work. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID001788



Screenshot 48 - Server roles detected and list of components to install.

7. A list of the Microsoft Exchange Server 2007/2010 server roles detected and GFI MailEssentials components required is displayed. Click **Next** to install the required GFI MailEssentials components.

8. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

4.5 Installing on an email gateway or relay/perimeter server

Introduction

GFI MailEssentials can be installed:

- On a perimeter server (e.g. DMZ) with Microsoft Exchange Server 2007/2010 in Edge Server role.
- As a mail relay server between the perimeter (gateway) SMTP server and the recipients' inboxes with Microsoft Exchange Server 2007/2010 in Hub Transport role.

Both setups enable you to reduce unnecessary email traffic by using your Active Directory resources (at a perimeter/gateway server level) to drop connections of non-existent email recipients in incoming email. This greatly helps against common spamming techniques such as Directory Harvest Attacks (a brute force type of attack used by spammers to find valid/existent e-mail addresses at a domain). This structure eliminates most spam from arriving at your Microsoft Exchange server.

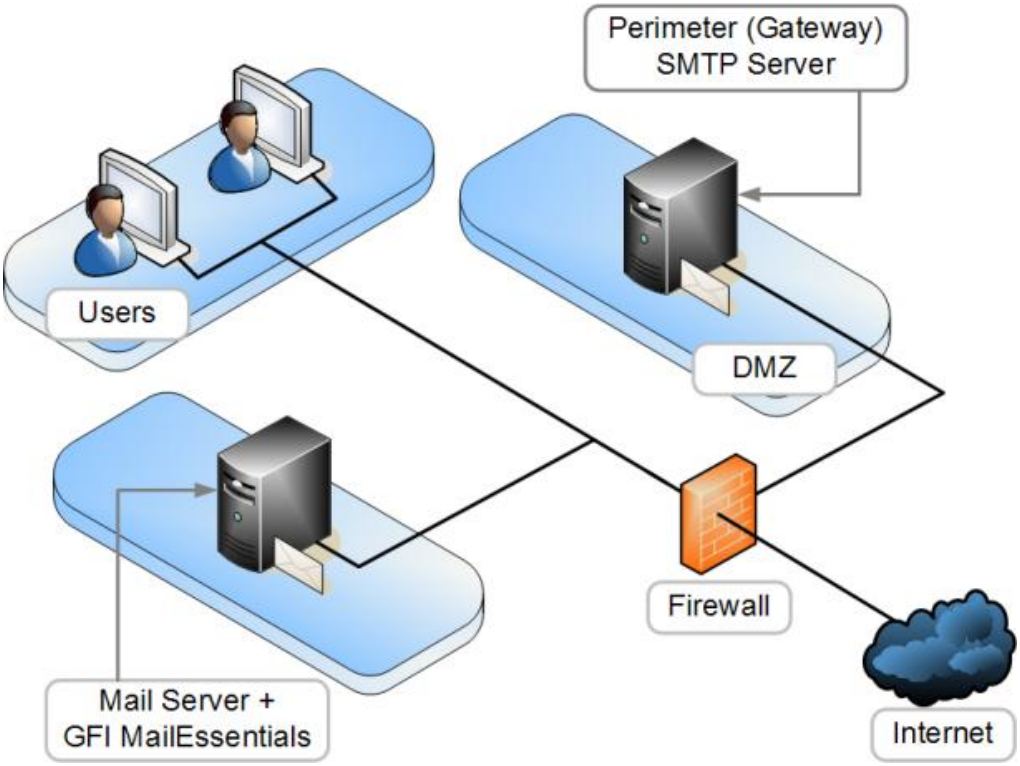


Figure 4 - A typical Perimeter SMTP Relay Server setup

4.5.1 Pre-install actions

Step 1: Send and Receive connector setup

NOTE: These connectors are not required for Microsoft Exchange Server 2007/2010 installed with Edge Server Role.

Ensure that the required Send connectors and Receive connectors to and from Microsoft Exchange 2007/2010 are created for servers installed with Hub Transport Role.

Where these are not yet created:

1. Add a 'Send Connector' to Microsoft Exchange server to forward all emails to the GFI MailEssentials machine

- From the Microsoft Exchange Server Management Console select **Organization Configuration ► Hub Transport ► Actions ► New Send Connector**
- In the New SMTP connector wizard, key in the name for the connector in the introduction screen.

  NOTE: You can use 'GFI MailEssentials SMTP Connector'.
- From the Select the intended use for this Send Connector drop down list box select **Internet**.
- From the Address space screen click **Add** and key in *****. Click **Ok** and click **Next**.
- Choose **Route mail through the following smart host**, click **Add** and specify the **IP address** of the server where GFI MailEssentials is installed. Click **Next**.
- Set the authentication for the GFI MailEssentials machine (if

required) and click **Next**.

- Select the Hub Transport server with which this connector will be associated and click **Next**.
- Verify the configuration summary and click **New** to create the new send connector.

NOTE: On completion, the GFI MailEssentials connector will be available in the **Send Connectors** tab and is enabled by default.

2. Add a 'Receive Connector' to Microsoft Exchange server to accept emails from the GFI MailEssentials Machine

- From the Exchange Management Shell, key in the following command:

```
new-receiveconnector -name "GFI MailEssentials" -
Bindings       "0.0.0.0:25"       -RemoteIPRanges
"<MailEssentials   IP   Address>"   -AuthMechanism
"ExternalAuthoritative"         -PermissionGroups
"ExchangeServers"
```

Change <MailEssentials IP Address> with the IP address of the GFI MailEssentials machine. Example:

```
new-receiveconnector -name "GFI MailEssentials" -
Bindings       "0.0.0.0:25"       -RemoteIPRanges
"192.168.0.1"                      -AuthMechanism
"ExternalAuthoritative"         -PermissionGroups
"ExchangeServers"
```

Step 2: Test your new mail relay server

Before installing GFI MailEssentials, verify that your new mail relay server is working correctly:

Test SMTP inbound connection via test email

1. Send an email from an 'external' account (e.g. Gmail) to an internal email address/user.

2. Ensure that intended recipient received the test email in the respective email client.

Test SMTP outbound connection via test email

1. Send an email from an 'internal' email account to an external account (e.g. Gmail)

2. Ensure that the intended recipient/external user received the test email.

NOTE: You can also use 'Telnet' to manually send the test email and obtained more troubleshooting information. For more information refer to:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

4.5.2 Upgrades from earlier version

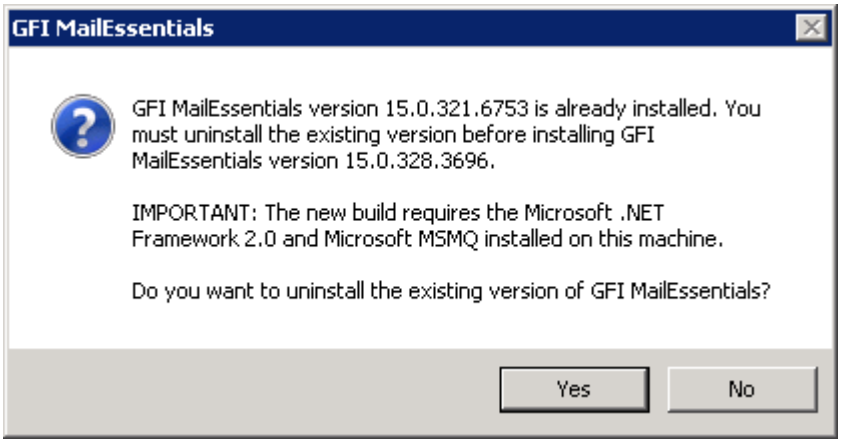
If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

Important notes

- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.
- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com
- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. NO DATA WILL BE LOST.

4.5.3 Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 49 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to New installations section below.

4.5.4 New installations

Important notes

1. During installation, GFI MailEssentials restarts Microsoft Exchange Server services. This is required to allow GFI MailEssentials components to be registered and started.

2. Before starting installation, close any running Windows applications.

Installation procedure

1. Logon to your Microsoft Exchange Server machine using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

3. Select install language and click **Next**.

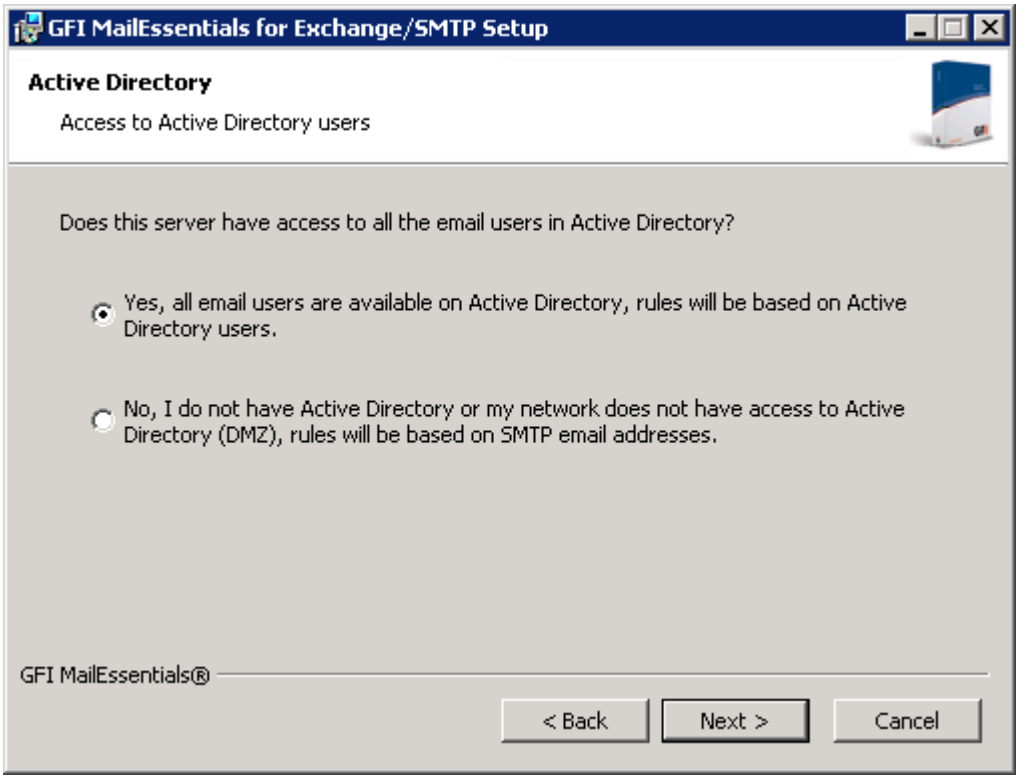
4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

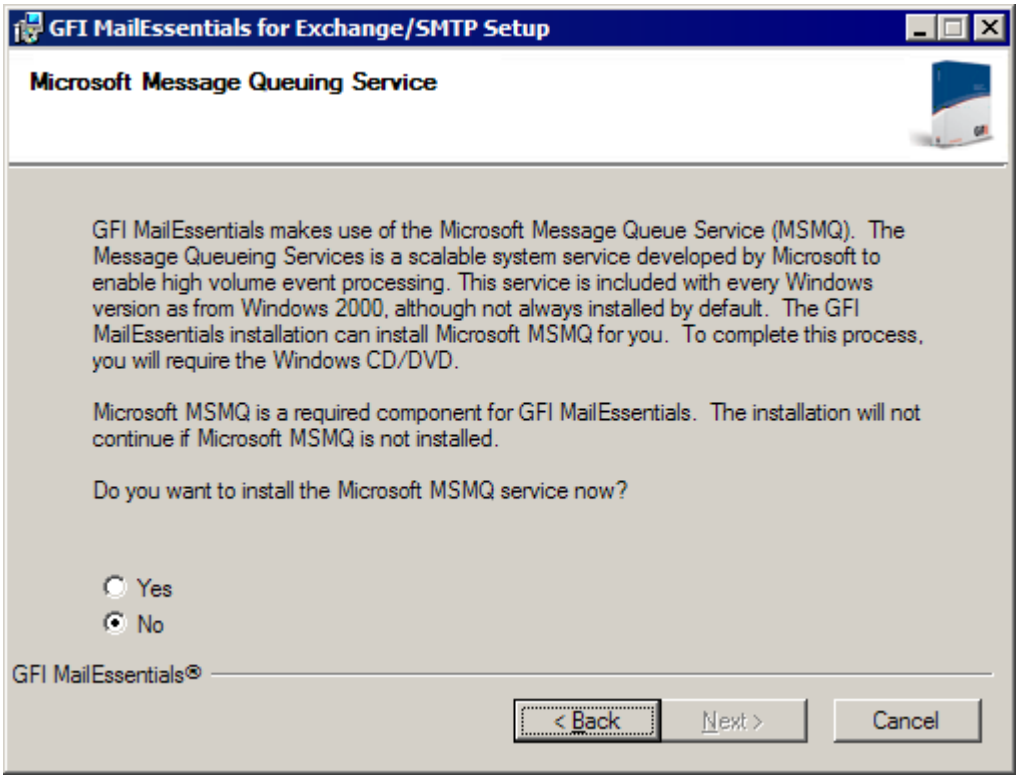
7. Specify user details and enter license key. Click **Next** to continue.

8. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 50 - Selecting SMTP mode or Active Directory mode

9. Specify whether GFI MailEssentials will get the list of email users (required for user-based configuration/rules e.g. disclaimers) from Active Directory or SMTP server. Click **Next** to continue.


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 51 - Installing Microsoft Message Queuing Service

10. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

11. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service.

  IMPORTANT: Failing to restart the SMTP service <u>will negatively affect</u> anti spam filtering and email flow.

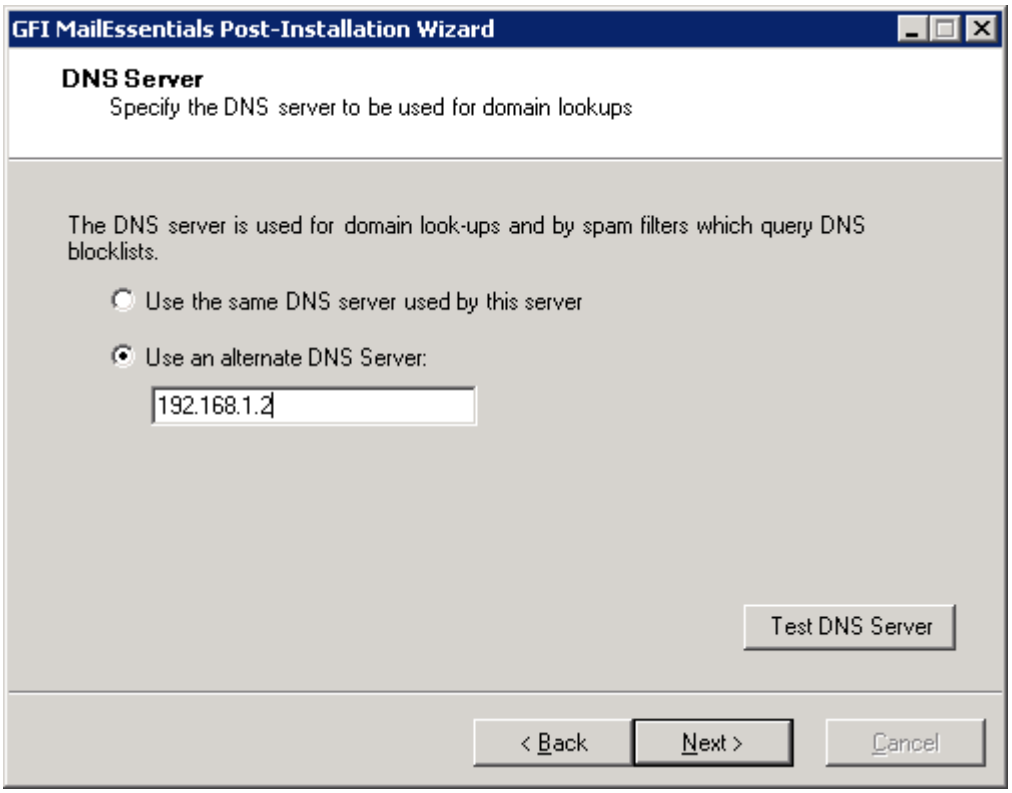
- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

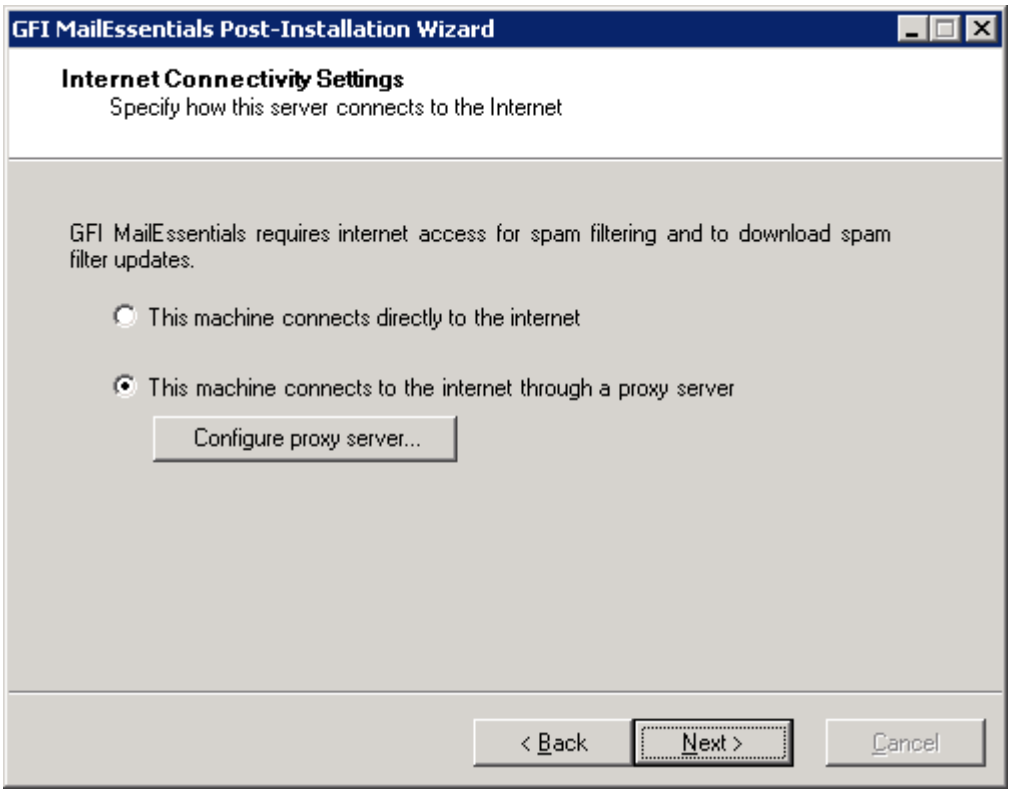

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 52 - DNS Server settings

2. In the **DNS Server** dialog, select:

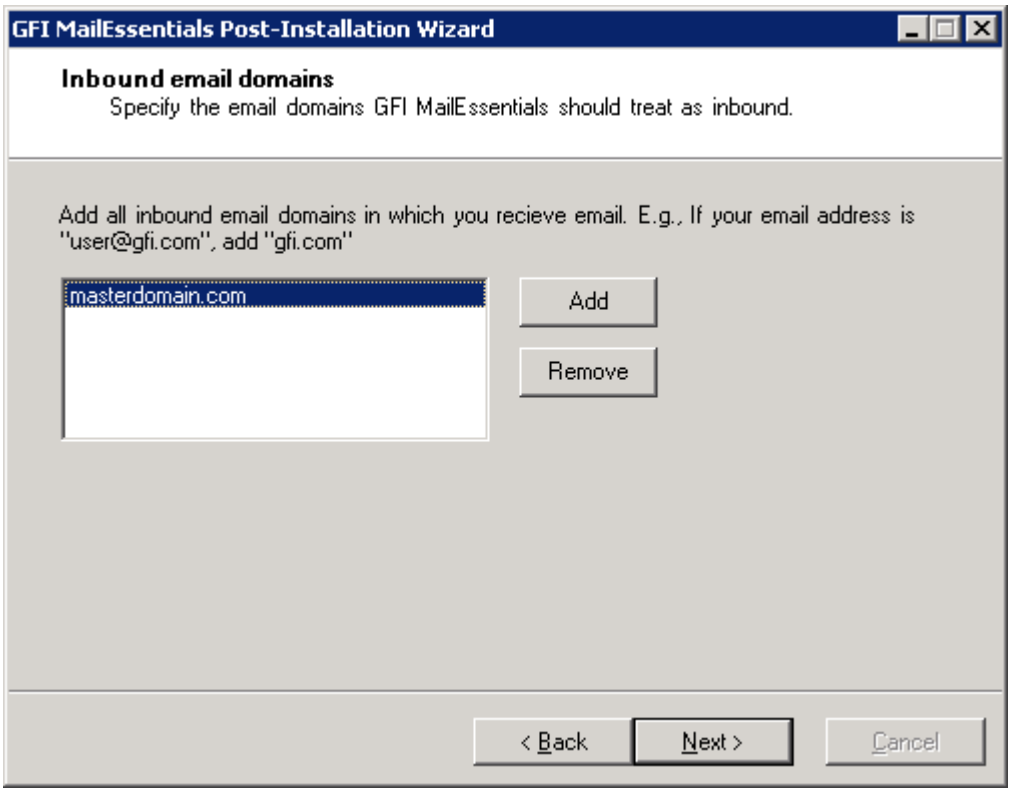
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 53 - Internet connectivity settings

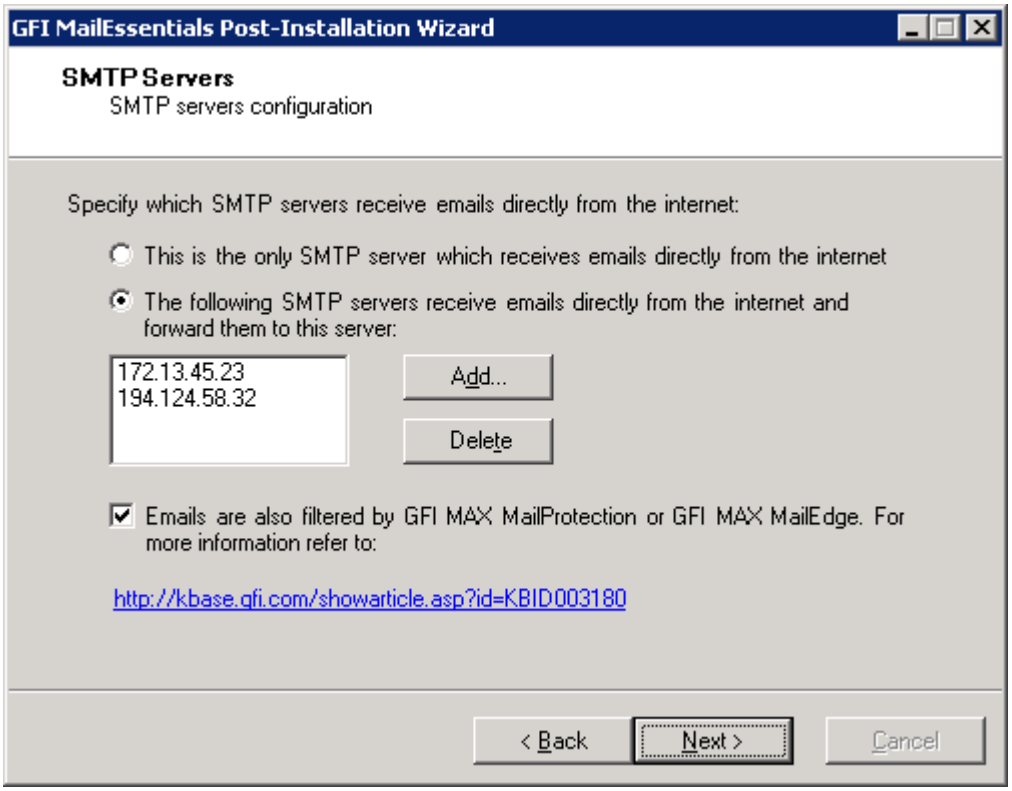
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 54 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 55 - SMTP Server settings

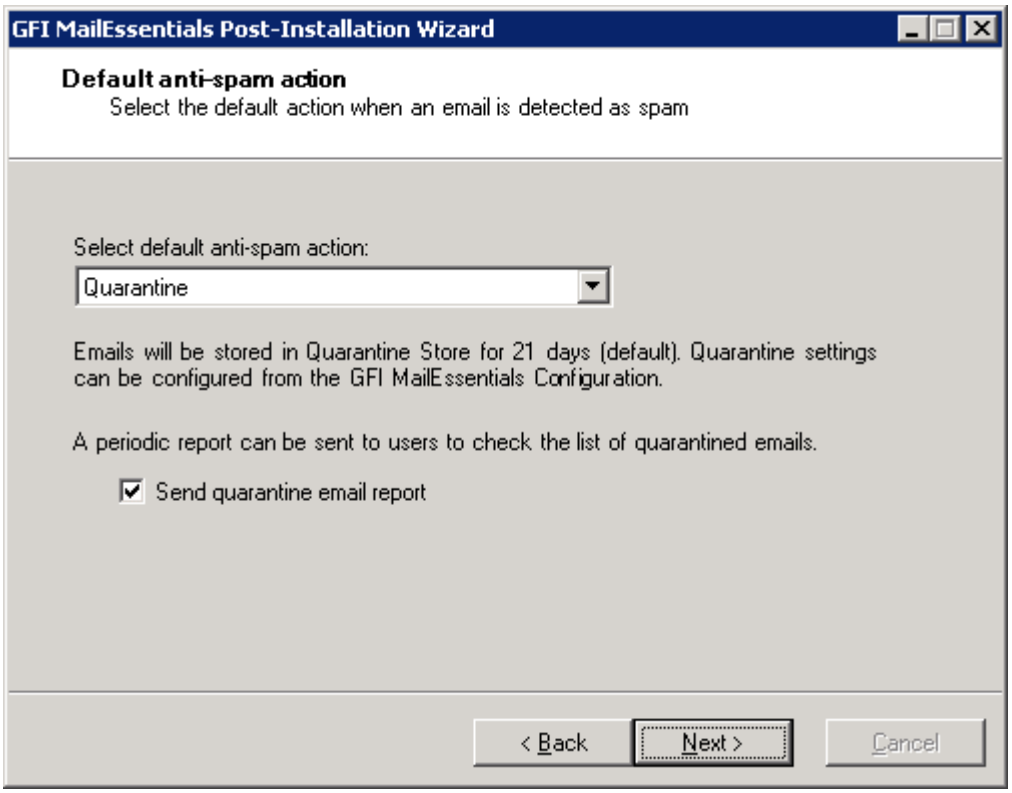
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.

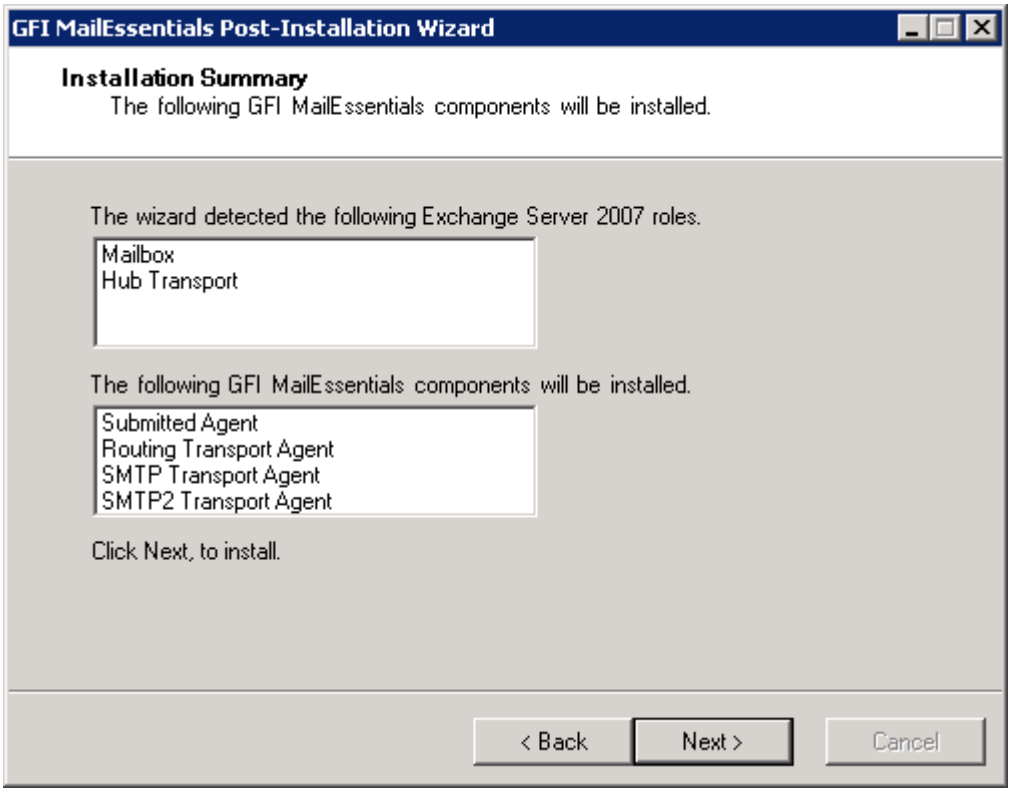

GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 56 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

NOTE: When installing on Microsoft Exchange 2010 and the default action selected is **Move to mailbox sub-folder**, a user with impersonation rights must be created. Select whether to let GFI MailEssentials automatically create the user or manually specify the credentials and click **Set impersonation rights** to assign the required rights to the specified user. This user must be dedicated to this feature only and the credentials must not be changed, otherwise the Move to Exchange folder feature will not work. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID001788



Screenshot 57 - Server roles detected and list of components to install.

7. A list of the Microsoft Exchange Server 2007/2010 server roles detected and GFI MailEssentials components required is displayed. Click **Next** to install the required GFI MailEssentials components.

8. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

4.6 Installing on Microsoft Exchange Server 2007 clusters

On Microsoft Exchange 2007 servers only servers with the Mailbox Role can be part of a cluster. Any other roles are required to be installed on separate servers.

To install GFI MailEssentials as part of a Microsoft Exchange 2007 cluster, install GFI MailEssentials on a server running the Hub Transport or the Edge Transport Role. Alternatively, you install GFI MailEssentials on a separate machine in gateway/perimeter server mode.

- On Microsoft Exchange 2007 server clusters without the Mailbox role, the option to move SPAM to subfolders of the users' mailbox is disabled.
- High availability for the Hub Transport, Edge Transport, Client Access, and Unified Messaging server roles is achieved through a combination of server redundancy, Network Load Balancing (NLB), hardware load balancing, Domain Name System (DNS) round robin, as well as proactive server, service, and infrastructure management. In this case GFI MailEssentials will need to be installed on all servers running the Hub Transport roles or all

servers running the Edge Transport roles.

Instructions on how to install GFI MailEssentials are provided in the previous sections.

5 Installation for Lotus Domino

5.1 Introduction

Installing GFI MailEssentials with Lotus Domino enables you to scan all inbound emails received from 'outside' (i.e. the internet) for spam before reaching your Lotus Domino server. Outbound emails relayed to GFI MailEssentials are also processed (e.g. adding of disclaimers and auto-whitelisting) before these are sent via internet.

To install GFI MailEssentials with Lotus Domino, the server where GFI MailEssentials is installed must be configured as an email gateway server (also known as "Smart host" or "Mail relay" server) for all your email. All inbound and outbound email must pass through this server for scanning before being relayed to the mail server for distribution.

5.2 System requirements

5.2.1 Software

Supported operating systems

- Microsoft Windows Server 2008 (x86 or x64)
- Microsoft Windows Server 2003 Standard/Enterprise (x86 or x64)

Mail Servers

- Lotus Domino 6 or later

Other components

- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 - included by default on Windows Server 2003 or later. This can be downloaded from:

  http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en
- Internet Information Services (IIS) (x32 or x64) - SMTP service and WWW service.
- Microsoft XML core services: For UK/US English OS this is installed automatically by GFI MailEssentials. For other languages, this can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- Microsoft Message Queuing Services.

5.2.2 Hardware

Processor

- **Minimum:** Intel Pentium or compatible 1 GHz 32-bit processor
- **Recommended:** x64 architecture-based server with Intel 64 architecture or AMD64 platform.

Memory

- **Minimum:** 1GB
- **Recommended:** 2GB RAM

Physical Storage

- **Minimum:** 500MB for installation, 2GB for execution.
- **Recommended:** 500MB for installation, 4GB for execution

5.3 Important settings

5.3.1 Antivirus and backup software

Antivirus and backup software may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials.

Disable third party antivirus and backup software from scanning the following folders:

x86 installations (32-bit)	x64 installations (64-bit)
<..*Program Files\GFI\MailEssentials*>	<..*Program Files (x86)\GFI\MailEssentials*>
<..*Program Files\Common Files\GFI*>	<..*Program Files (x86)\Common Files\GFI*>
<..*Inetpub\mailroot*> If installed on a gateway machine.	

5.3.2 Firewall port settings

Configure your firewall to allow the following port connections. These ports are used by GFI MailEssentials to connect to GFI servers:

- **DNS (Port 53)** - Used by anti spam filters (IP DNS Blocklist, Sender Policy Framework, Header Checking).
- **FTP (Ports 20 and 21)** - Used by GFI MailEssentials to connect to 'ftp.gfisoftware.com' and retrieve latest product version information.
- **HTTP (Port 80) -** Used by GFI MailEssentials to download product patch and anti spam filter updates (i.e. SpamRazer, Anti-Phishing, and Bayesian anti spam filters) from the following locations:
  - 'http://update.gfi.com'
  - 'http://update.gfisoftware.com'
  - 'http://support.gfi.com

- 'http://db11.spamcatcher.net' (GFI MailEssentials 14 or earlier)
- 'http://sn92.mailshell.net' (GFI MailEssentials 14 SR1 or later)

- **Remoting (Ports 8021)** - Used in the latest builds of GFI MailEssentials for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server.

  NOTE: Ensure that no other applications (except GFI MailEssentials) are listening on port 8021.
- **LDAP (Port 389)** - Used by GFI MailEssentials to get email addresses from Lotus Domino server.

5.4 Installing on gateway servers for Lotus Domino

5.4.1 Pre-install actions

GFI MailEssentials uses the IIS SMTP service as its SMTP Server and therefore the IIS SMTP service must be configured to act as a mail relay server. This is achieved as follows:

Step 1: Enable IIS SMTP Service

Windows Server 2003

1. Go to **Start ► Control Panel ► Add or Remove Programs ► Add/Remove Windows Components**.
2. Select **Internet Information Services (IIS)** and click **Details**.
3. Select the **SMTP Service** option and click **OK**.
4. Click **Next** to finalize your configuration.

Windows Server 2008

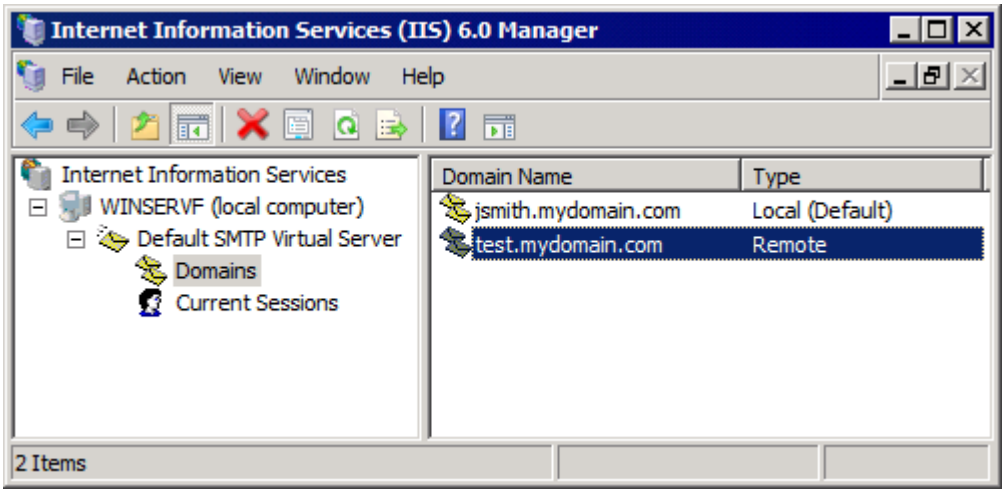
1. Launch the Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server** checkbox.

NOTE: The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize the configuration.

Step 2: Create SMTP domain(s) for email relaying

1. Go to **Start ► Control Panel ► Administrative Tools**.
2. Click on **Internet Information Services (IIS) Manager**.



Screenshot 58 - Internet Information Services (IIS) Manager

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

4. Select the IP address currently assigned to your SMTP server and click **OK**.

5. Expand the **Default SMTP Virtual Server** node.

6. Right click **Domains** and select **New ► Domain**.

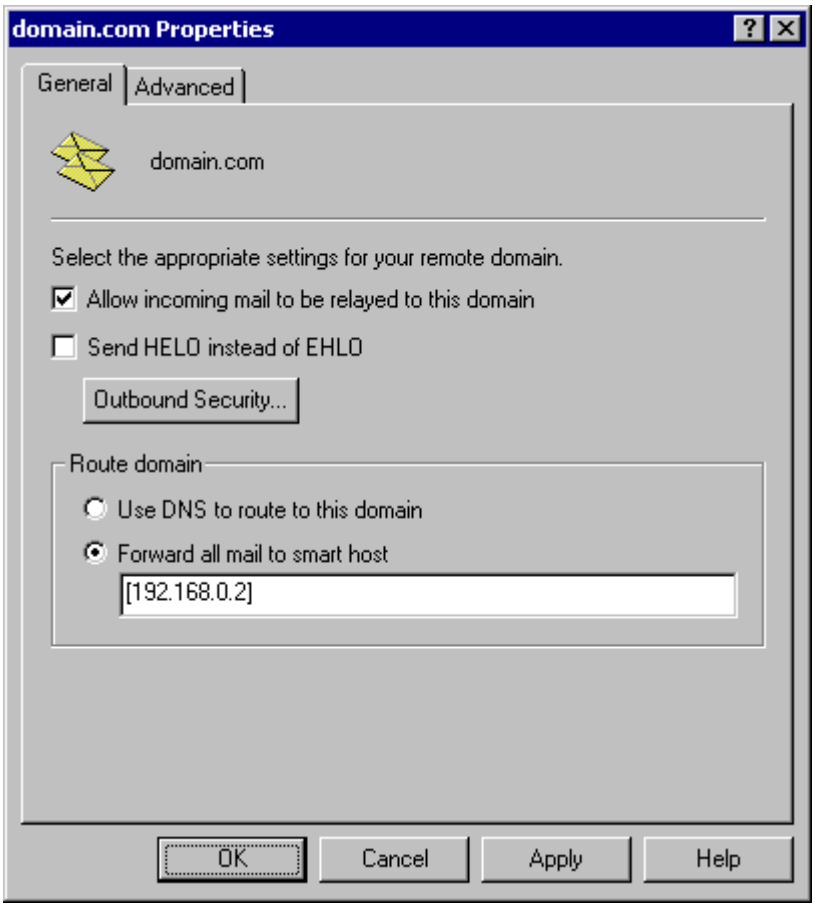
7. Select the **Remote** option and click **Next**.

8. Specify domain name (e.g. test.gfi.com) and click **Finish**.

Step 3: Enable email relaying to your Microsoft Exchange server:

1. Right click on the new domain (e.g. test.gfi.com) and select **Properties**.

2. Select the **Allow the Incoming Mail to be Relayed to this Domain** checkbox.



Screenshot 59 - Configure the domain

3. Select the **Forward all mail to smart host** option and specify the IP address of the server managing emails in this domain. IP address must be enclosed in square brackets e.g. [123.123.123.123] so to exclude them from all DNS lookup attempts.

4. Click **OK** to finalize your configuration.

Step 4: Secure your SMTP email-relay server

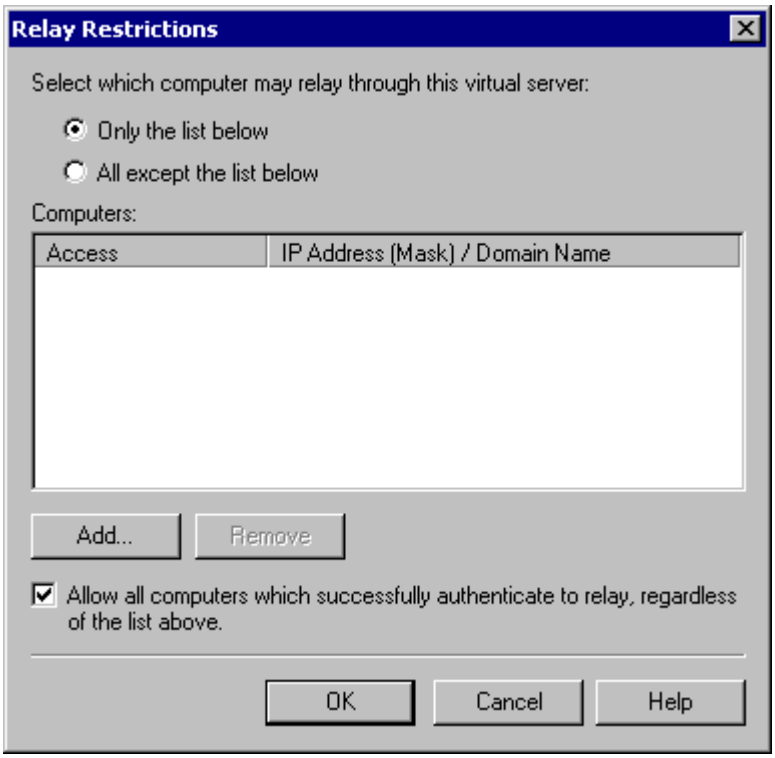
If unsecured, your mail relay server can be exploited and used as an open relay for spam. To avoid this from happening, it is recommended that you specifically define which mail servers can route emails through this mail relay server (i.e. allow only specific servers to use this email relaying setup). To achieve this:

1. Go to **Start ► Control Panel ► Administrative Tools**.

2. Click on **Internet Information Services (IIS) Manager**.

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

4. Click on the **Access** tab and select **Relay**.



Screenshot 60 - Relay options

5. Select the **Only the list below** option and click **Add**.

6. Specify IP(s) of the mail server(s) that are allowed to route emails through your mail relay server. You can specify:

- **Single computer -** i.e. Authorize one specific machine to relay email through this server. Use the **DNS Lookup** button to lookup an IP address for a specific host.
- **Group of computers -** i.e. Authorize specific computer(s) to relay emails through this server.
- **Domain -** Allow all computers in a specific domain to relay emails through this server.

  NOTE: The Domain option adds a processing overhead that can degrade SMTP service performance. This is due to the reverse DNS lookup processes triggered on all IP addresses (within that domain) that try to route emails through this relay server.

Step 5: Configure Lotus Domino for GFI MailEssentials

a. Configure Lotus Domino to send outbound emails through GFI MailEssentials

1. From the 'Lotus Domino Administrator', click **Configuration** tab and select **configurations** item under the **server** node.

2. From the 'Configurations main window, select the server to use with GFI MailEssentials and click **edit configuration**.

3. Select **Router/SMTP** tab and ensure **Basics** is selected.

4. Double click on the content to edit. Select **Relay host for messages leaving the local internet domain** option and key in the IP address of the mail gateway server where GFI MailEssentials is installed.

5. Click **Save and Close** to save configuration.

b. Configure Lotus Domino LDAP settings

1. From the 'Directory Assistance database', click on **Add directory assistance** to create a new Assistance document.

2. Select the **LDAP Clients** checkbox from the 'Make this domain available to:' option.

3. From the 'server configuration', edit the credentials under the configuration. Enable **Anonymous** authentication to allow GFI MailEssentials to access Lotus Domino LDAP.

Step 6: Update your domain MX record to point to mail relay server

Update the MX record of your domain to point to the IP of the new mail relay server. If your DNS server is managed by your ISP, ask your ISP to update the MX record for you.

If MX record is not updated all emails will be routed directly to your email server - hence by-pass GFI MailEssentials anti spam filters.

Verify that MX record has been successfully updated

To verify whether MX record is updated:

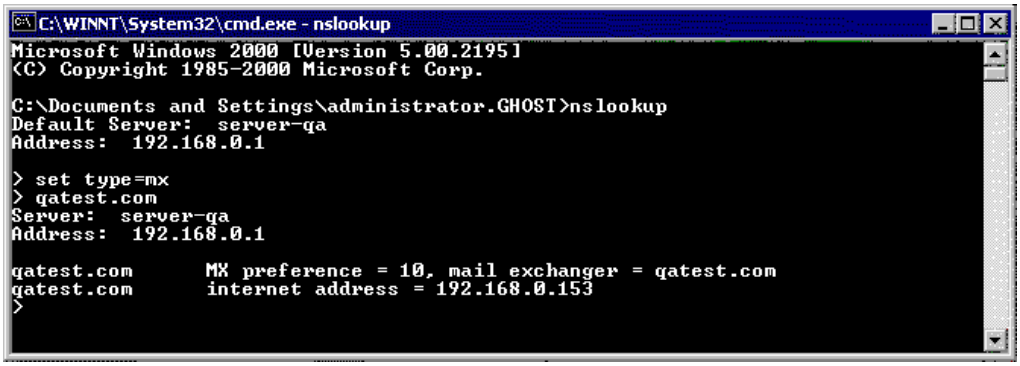
1. Click **Start ► Run** and type **Command**

2. From the command prompt type in: **nslookup**

3. Type in: **set type=mx**

4. Specify your mail domain name.

The MX record should return the IP addresses of the mail relay servers.



Screenshot 61 - Checking the MX record of your domain

Step 7: Test your new mail relay server

Before proceeding to install GFI MailEssentials, verify that your new mail relay server is working correctly by doing as follows:

Test IIS SMTP inbound connection via test email

1. Send an email from an 'external' account (e.g. Gmail) to an internal email address/user.

2. Ensure that intended recipient received the test email in the respective email client.

Test IIS SMTP outbound connection via test email

1. Send an email from an 'internal' email account to an external account (e.g. Gmail)

2. Ensure that the intended recipient/external user received the test email.

NOTE: You can also use 'Telnet' to manually send the test email and obtained more troubleshooting information. For more information refer to:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

5.4.2 Upgrade from earlier version

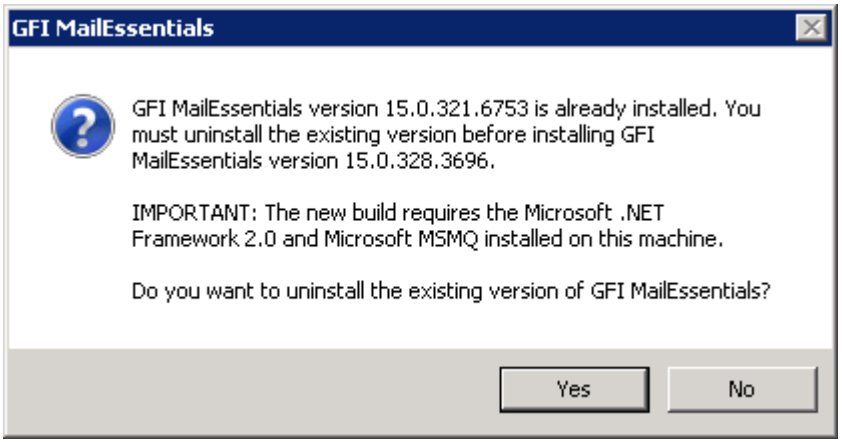
If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

Important notes

- Upgrades cannot be undone i.e. you cannot downgrade to an earlier version once you have installed the latest version.
- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com.
- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. NO DATA WILL BE LOST.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 62 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen

instructions. For assistance refer to New installations section below.

5.4.3 New installations

Important notes

1. During installation, GFI MailEssentials restarts IIS services. This is required to allow GFI MailEssentials components to be registered and started.

2. Before starting installation, close any running Windows applications.

Installation procedure

1. Logon to the email gateway server where GFI MailEssentials will be installed using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

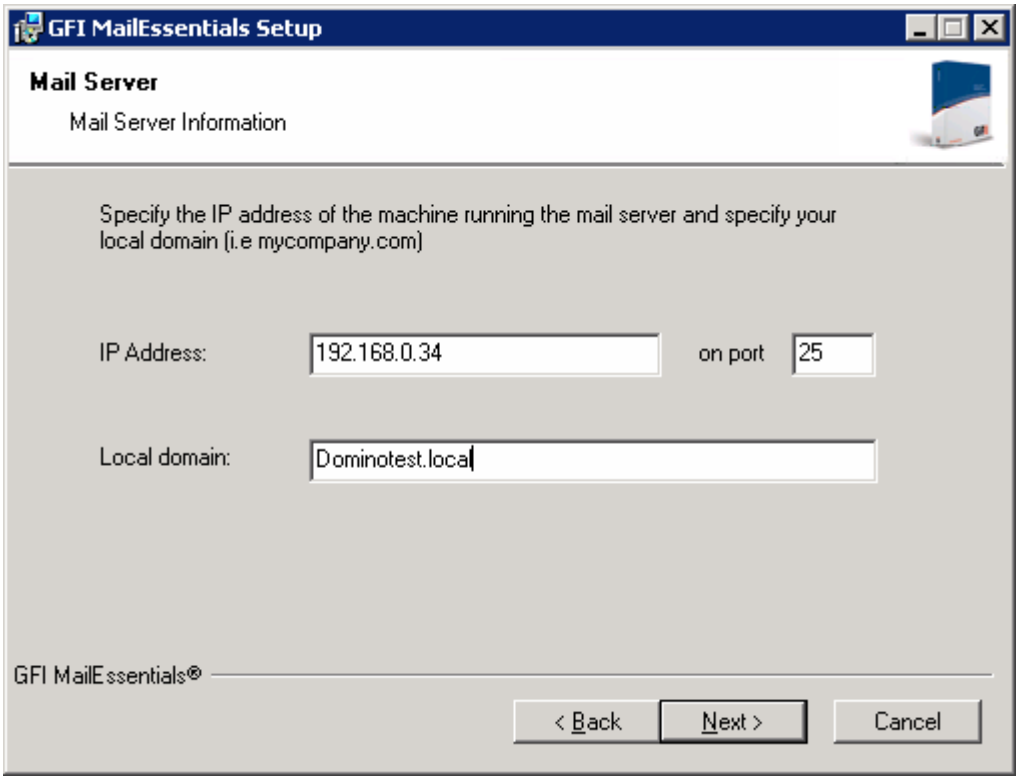
3. Select install language and click **Next**.

4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

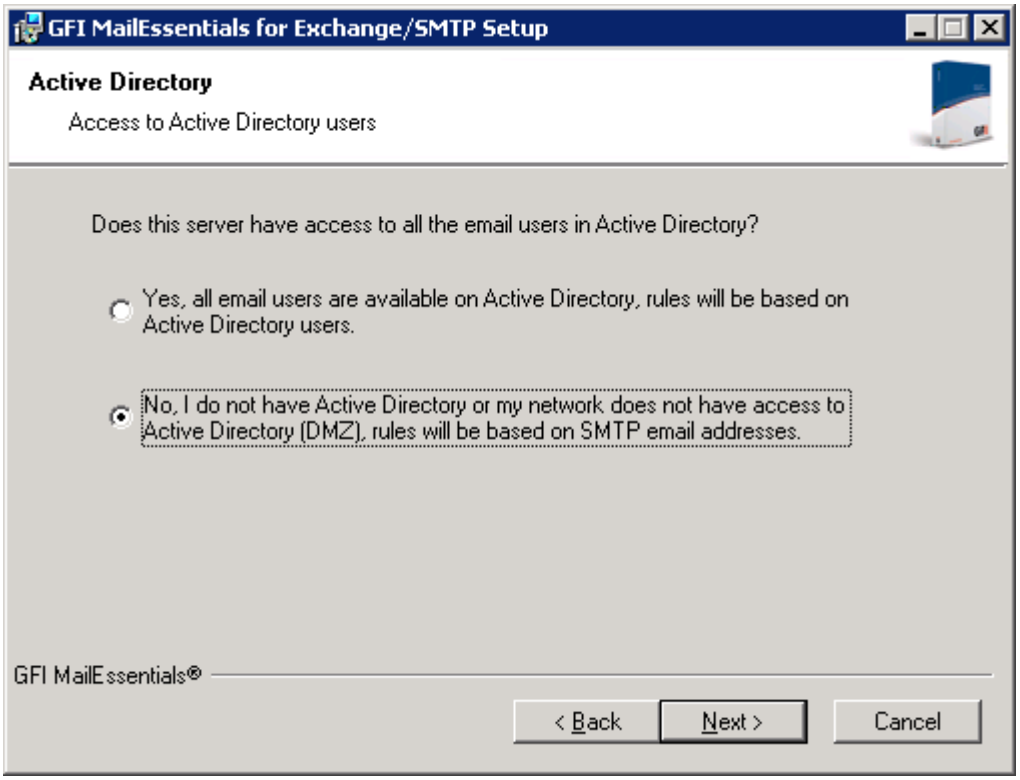
7. Specify user details and enter license key. Click **Next** to continue.



Screenshot 63 - Specify mail server details

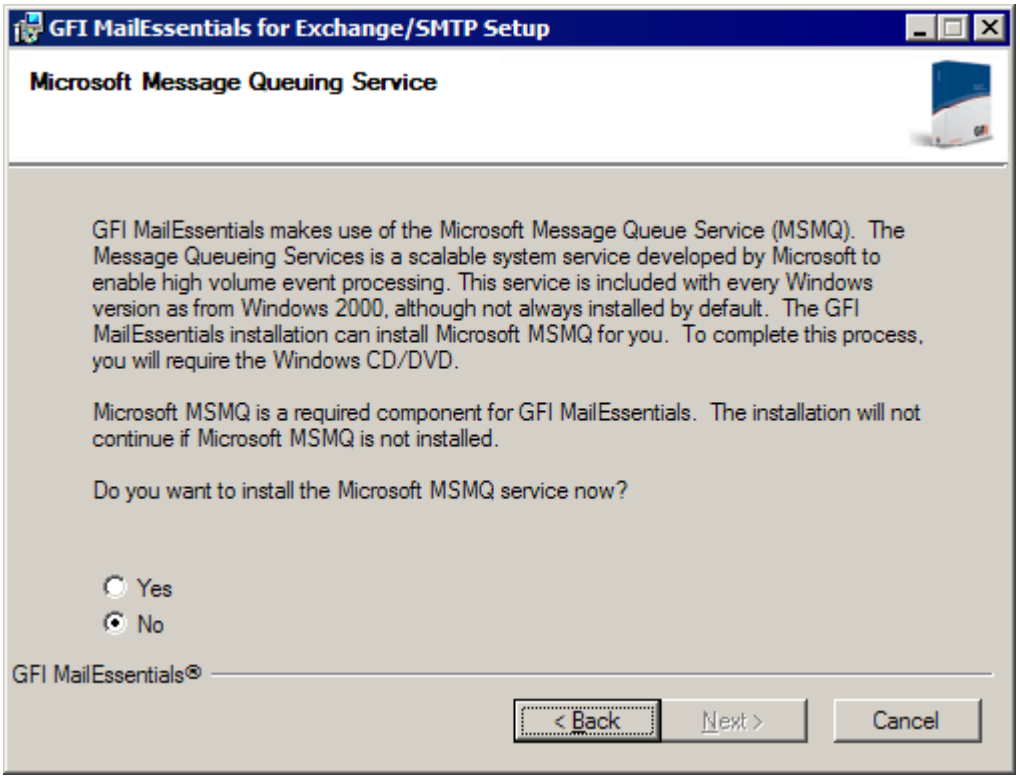
8. Specify IP address and listening port of Lotus Domino Server and the external domain name used. Click **Next** to continue.

9. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 64 - Selecting SMTP mode

10. Select **No, I do not have Active Directory…** option to use SMTP server to get the list of email users. Click **Next** to continue**.**


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 65 - Installing Microsoft Message Queuing Service

11. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install MSMQ. Click **Next** to continue.

12. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service.

  IMPORTANT: Failing to restart the SMTP service will negatively affect anti spam filtering and email flow.

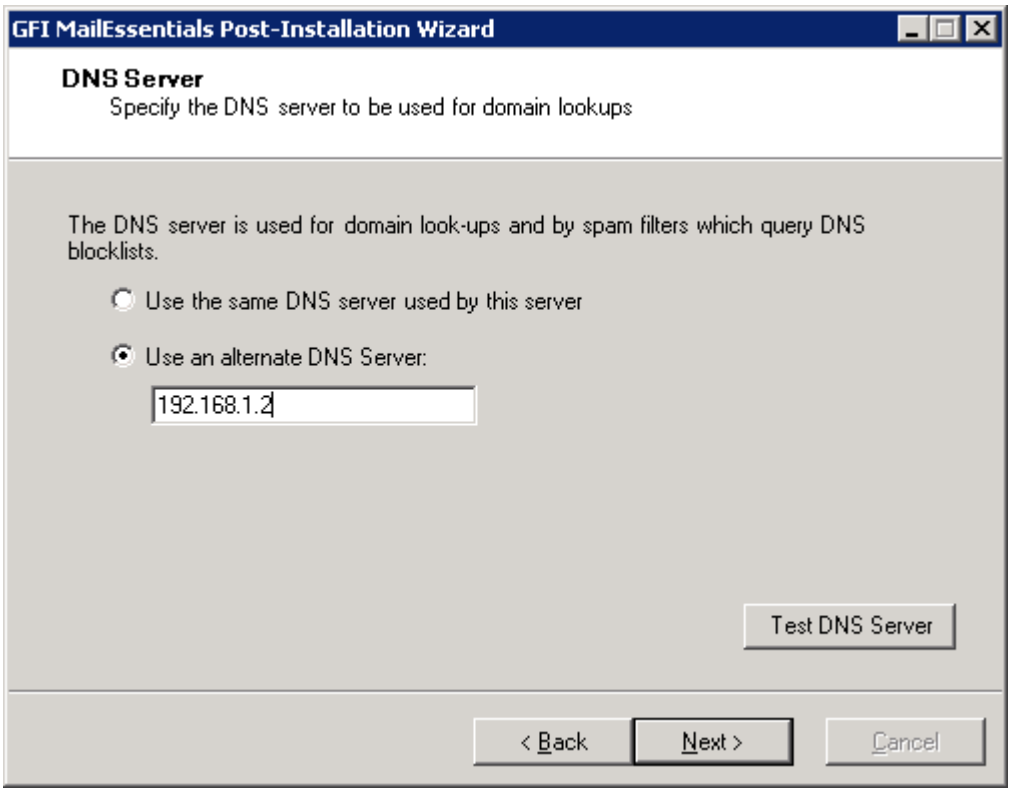
- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.


GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

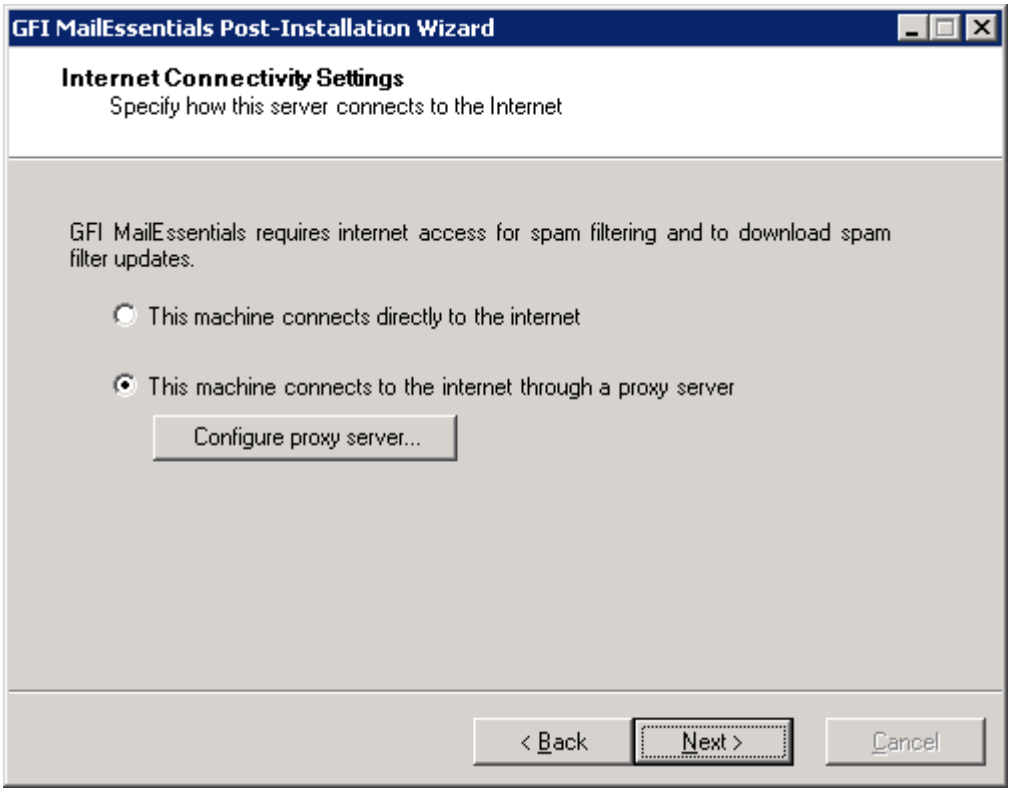
Screenshot 66 - DNS Server settings

2. In the **DNS Server** dialog, select:

- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

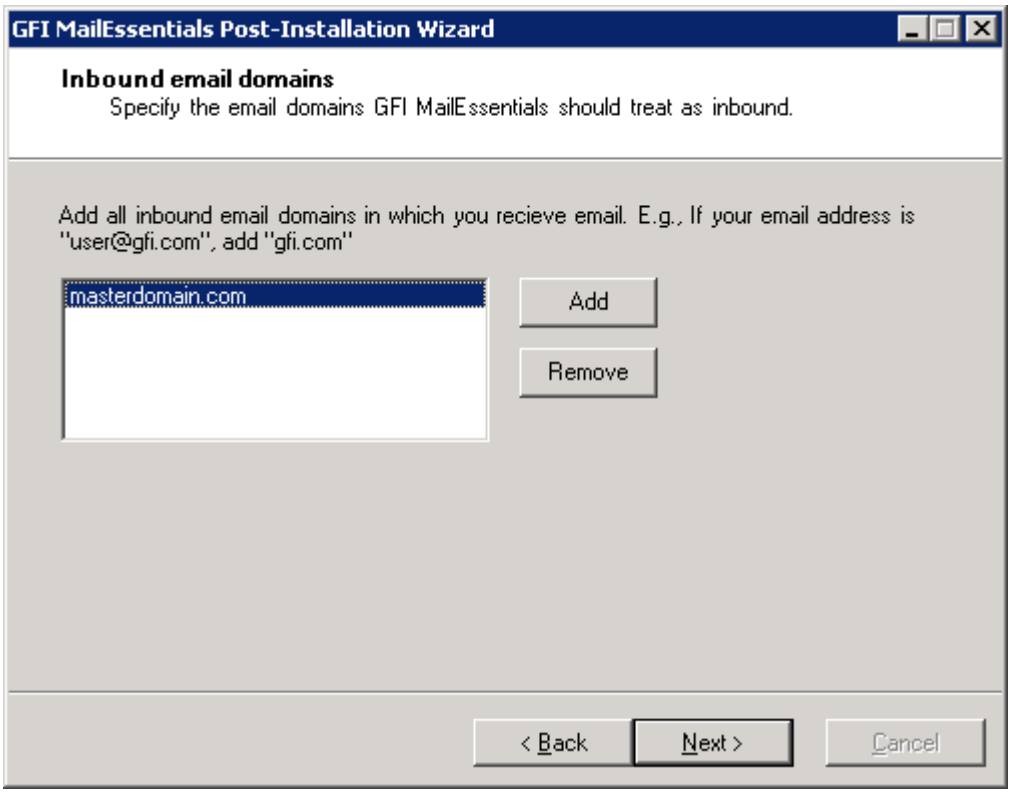
Click **Test DNS Server** to test connection with the specified DNS

server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 67 - Internet connectivity settings

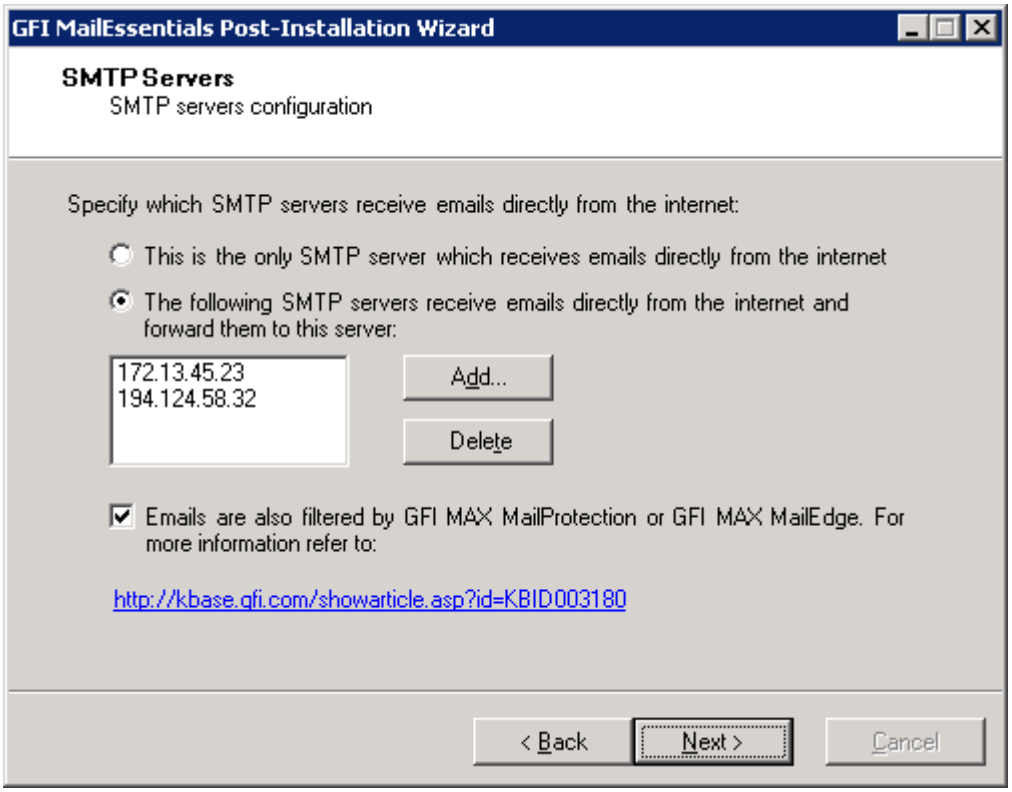
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 68 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 69 - SMTP Server settings

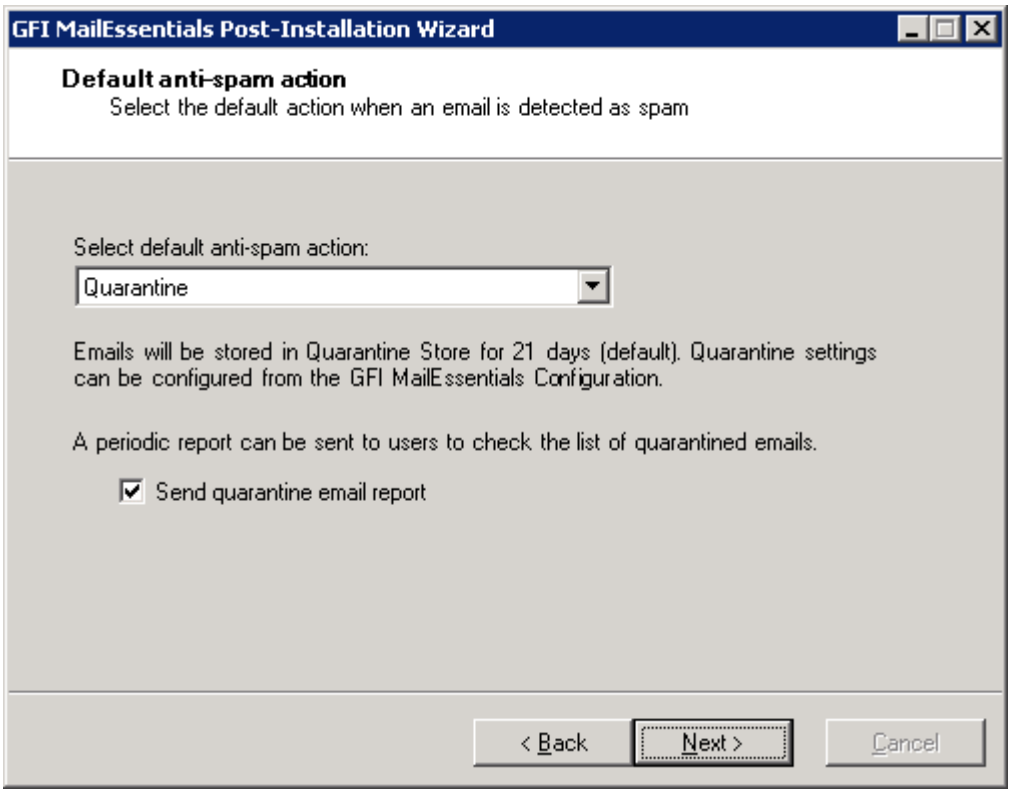
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 70 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

6 Installation for SMTP Servers

6.1 Introduction

Installing GFI MailEssentials with other SMTP servers enables you to scan all inbound emails received from 'outside' (i.e. the internet) for spam before reaching your SMTP Server. Outbound emails relayed to GFI MailEssentials are also processed (e.g. adding of disclaimers and auto-whitelisting) before these are sent via internet.

To install GFI MailEssentials with other SMTP servers, the server where GFI MailEssentials is installed must be configured as an email gateway server (also known as "Smart host" or "Mail relay" server) for all your email. All inbound and outbound email must pass through this server for scanning before being relayed to the mail server for distribution.

6.2 System requirements

6.2.1 Software

Supported operating systems

- Microsoft Windows Server 2008 (x86 or x64)
- Microsoft Windows Server 2003 Standard/Enterprise (x86 or x64)

Mail Servers

- Any SMTP compliant email server

Other components

- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 - included by default on Windows Server 2003 or later. This can be downloaded from:

  http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en
- Internet Information Services (IIS) (x32 or x64) - SMTP service and WWW service.
- Microsoft XML core services: For UK/US English OS this is installed automatically by GFI MailEssentials. For other languages, this can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- Microsoft Message Queuing Services.

6.2.2 Hardware

Processor

- **Minimum:** Intel Pentium or compatible 1 GHz 32-bit processor
- **Recommended:** x64 architecture-based server with Intel 64 architecture or AMD64 platform

Memory

- **Minimum:** 1GB
- **Recommended:** 2GB RAM

Physical Storage

- **Minimum:** 500MB for installation, 2GB for execution
- **Recommended:** 500MB for installation, 4GB for execution

6.3 Important settings

6.3.1 Antivirus and backup software

Antivirus and backup software may cause GFI MailEssentials to malfunction. This occurs when such software denies access to certain files required by GFI MailEssentials.

Disable third party antivirus and backup software from scanning the following folders:

x86 installations (32-bit)	x64 installations (64-bit)
<..\Program Files\GFI\MailEssentials>	<..\Program Files (x86)\GFI\MailEssentials>
<..\Program Files\Common Files\GFI>	<..\Program Files (x86)\Common Files\GFI>
<..\Inetpub\mailroot> If installed on a gateway machine.	

6.3.2 Firewall port settings

Configure your firewall to allow the following port connections. These ports are used by GFI MailEssentials to connect to GFI servers:

- **DNS (Port 53)** - Used by anti spam filters (IP DNS blocklist, Sender Policy Framework, Header Checking).
- **FTP (Ports 20 and 21)** - Used by GFI MailEssentials to connect to 'ftp.gfisoftware.com' and retrieve latest product version information.
- **HTTP (Port 80) -** Used by GFI MailEssentials to download product patch and anti spam filter updates (i.e. SpamRazer, Anti-Phishing, and Bayesian anti spam filters) from the following locations:
  - 'http://update.gfi.com'
  - 'http://update.gfisoftware.com'
  - 'http://support.gfi.com

- 'http://db11.spamcatcher.net' (GFI MailEssentials 14 or earlier)
- 'http://sn92.mailshell.net' (GFI MailEssentials 14 SR1 or later)

- **Remoting (Ports 8021)** - Used in the latest builds of GFI MailEssentials for inter-process communication. No firewall configuration is required to allow connections to or from the remoting ports since all the GFI MailEssentials processes run on the same server.

  NOTE: Ensure that no other applications (except GFI MailEssentials) are listening on port 8021.
- **LDAP (Port 389)** - Used by GFI MailEssentials to get email addresses from SMTP server.

6.4 Installing on gateway servers for SMTP Servers

6.4.1 Pre-install actions

GFI MailEssentials uses the IIS SMTP service as its SMTP Server and therefore the IIS SMTP service must be configured to act as a mail relay server. This is achieved as follows:

Step 1: Enable IIS SMTP Service

Windows Server 2003

1. Go to **Start ► Control Panel ► Add or Remove Programs ► Add/Remove Windows Components**.
2. Select **Internet Information Services (IIS)** and click **Details**.
3. Select the **SMTP Service** option and click **OK**.
4. Click **Next** to finalize your configuration.

Windows Server 2008

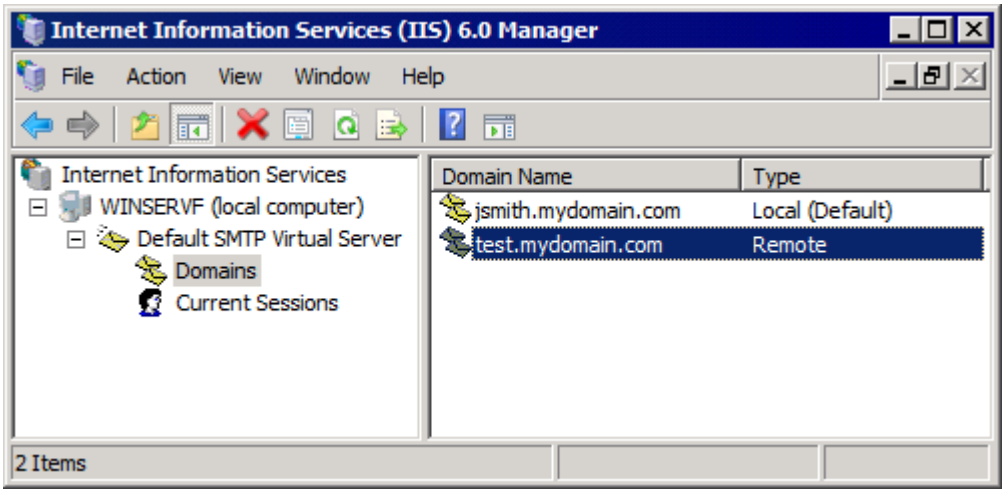
1. Launch the Windows Server Manager.
2. Navigate to the **Features** node and select **Add Features**.
3. From the **Add Features Wizard** select **SMTP Server** checkbox.

NOTE: The SMTP Server feature might require the installation of additional role services and features. Click **Add Required Role Services** to proceed with installation.

4. In the following screens click **Next** to configure any required role services and features, and click **Install** to start the installation.
5. Click **Close** to finalize the configuration.

Step 2: Create SMTP domain(s) for email relaying

1. Go to **Start ► Control Panel ► Administrative Tools**.
2. Click on **Internet Information Services (IIS) 6.0 Manager**.



Screenshot 71 - Internet Information Services (IIS) Manager

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

4. Select the IP address currently assigned to your SMTP server and click **OK**.

5. Expand the **Default SMTP Virtual Server** node

6. Right click **Domains** and select **New ► Domain**.

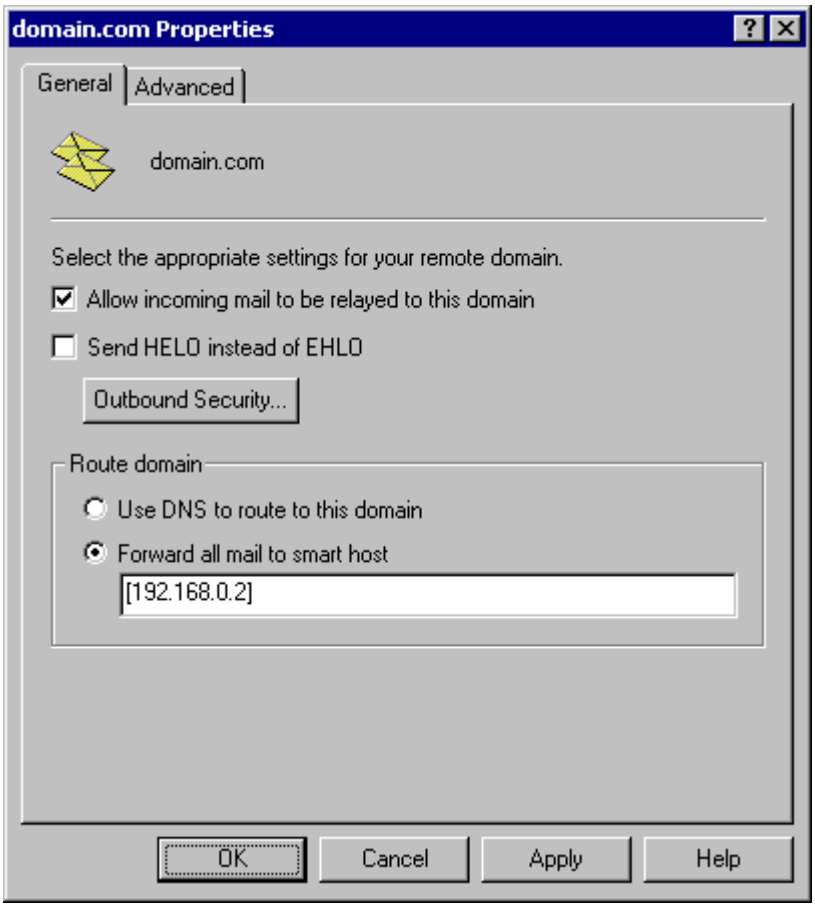
7. Select the **Remote** option and click **Next**.

8. Specify domain name (e.g. test.gfi.com) and click **Finish**.

Step 3: Enable email relaying to your remote SMTP server:

1. Right click on the new domain (e.g. test.gfi.com) and select **Properties**.

2. Select the **Allow the Incoming Mail to be Relayed to this Domain** checkbox.



Screenshot 72 - Configure the domain

3. Select the **Forward all mail to smart host** option and specify the IP address of the server managing emails in this domain. IP address must be enclosed in square brackets e.g. [123.123.123.123] so to exclude them from all DNS lookup attempts.

4. Click **OK** to finalize your configuration.

Step 4: Secure your SMTP email-relay server

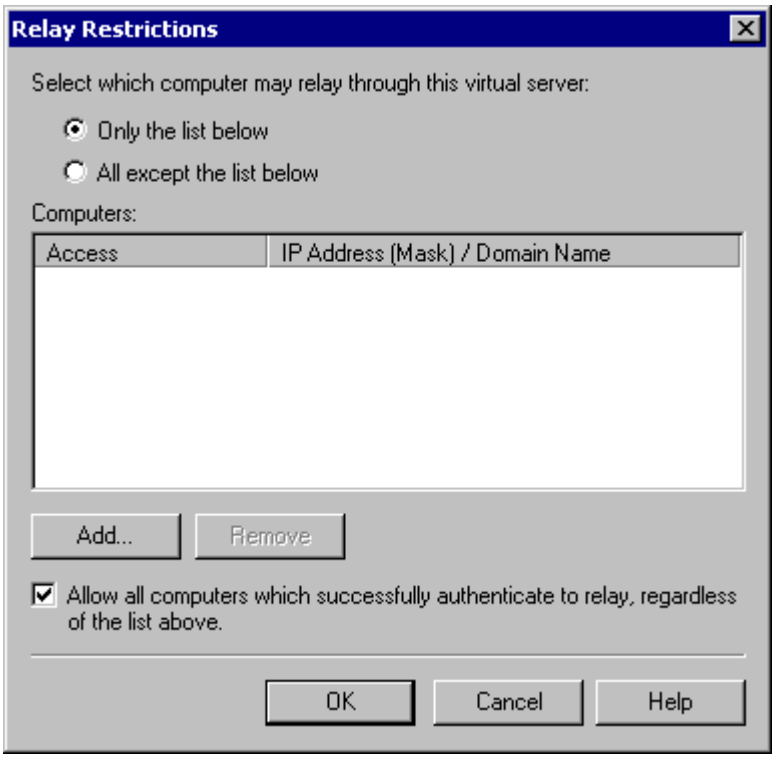
If unsecured, your mail relay server can be exploited and used as an open relay for spam. To avoid this from happening, it is recommended that you specifically define which mail servers can route emails through this mail relay server (i.e. allow only specific servers to use this email relaying setup). To achieve this:

1. Go to **Start ► Control Panel ► Administrative Tools**.

2. Click on **Internet Information Services (IIS) Manager**.

3. In the left pane, expand the respective server node. Right click on **Default SMTP Virtual Server** and select **Properties**.

4. Click on the **Access** tab and select **Relay**.



Screenshot 73 - Relay options

5. Select the **Only the list below** option and click **Add**.

6. Specify IP(s) of the mail server(s) that are allowed to route emails through your mail relay server. You can specify:

- **Single computer -** i.e. Authorize one specific machine to relay email through this server. Use the **DNS Lookup** button to lookup an IP address for a specific host.
- **Group of computers -** i.e. Authorize specific computer(s) to relay emails through this server.
- **Domain -** Allow all computers in a specific domain to relay emails through this server.

  NOTE: The Domain option adds a processing overhead that can degrade SMTP service performance. This is due to the reverse DNS lookup processes triggered on all IP addresses (within that domain) that try to route emails through this relay server.

Step 5: Configure your SMTP server for GFI MailEssentials

Refer to the SMTP server documentation on forwarding email to the GFI MailEssentials server.

Step 6: Update your domain MX record to point to mail relay server.

Update the MX record of your domain to point to the IP of the new mail relay server. If your DNS server is managed by your ISP, ask your ISP to update the MX record for you.

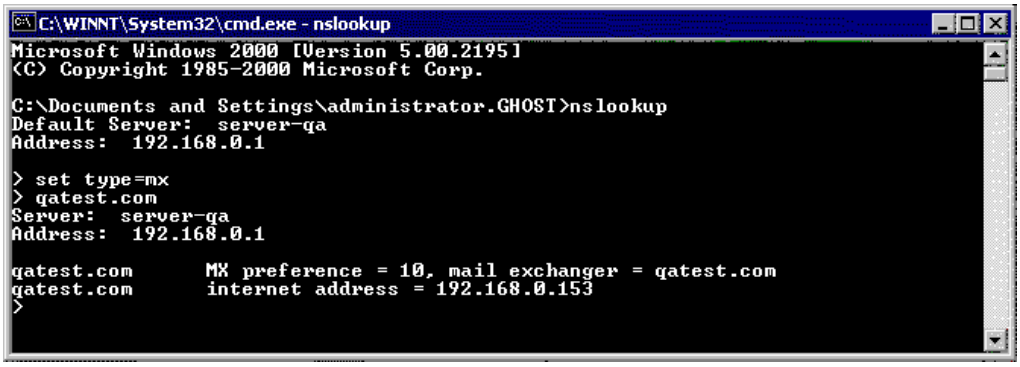
If the MX record is not updated, all emails will be routed directly to your email server - hence by-pass GFI MailEssentials anti spam filters.

Verify that MX record has been successfully updated

To verify whether MX record is updated do as follows:

1. Click **Start ► Run** and type in **Command**
2. From the command prompt type in: **nslookup**
3. Type in: **set type=mx**
4. Specify your mail domain name.

The MX record should return the IP addresses of the mail relay servers.



Screenshot 74 - Checking the MX record of your domain

Step 7: Test your new mail relay server

Before proceeding to install GFI MailEssentials, verify that your new mail relay server is working correctly by doing as follows:

Test IIS SMTP inbound connection via test email

1. Send an email from an 'external' account (e.g. Gmail) to an internal email address/user.

2. Ensure that intended recipient received the test email in the respective email client.

Test IIS SMTP outbound connection via test email

1. Send an email from an 'internal' email account to an external account (e.g. Gmail).

2. Ensure that the intended recipient/external user received the test email.

NOTE: You can also use 'Telnet' to manually send the test email and obtained more troubleshooting information. For more information refer to:

http://support.microsoft.com/support/kb/articles/Q153/1/19.asp

6.4.2 Upgrade from earlier version

If you are currently using a previous version of GFI MailEssentials (versions 9, 10, 11, 12 and 14), you can upgrade your current installation while at the same time retain all your existing configuration settings.

Important notes

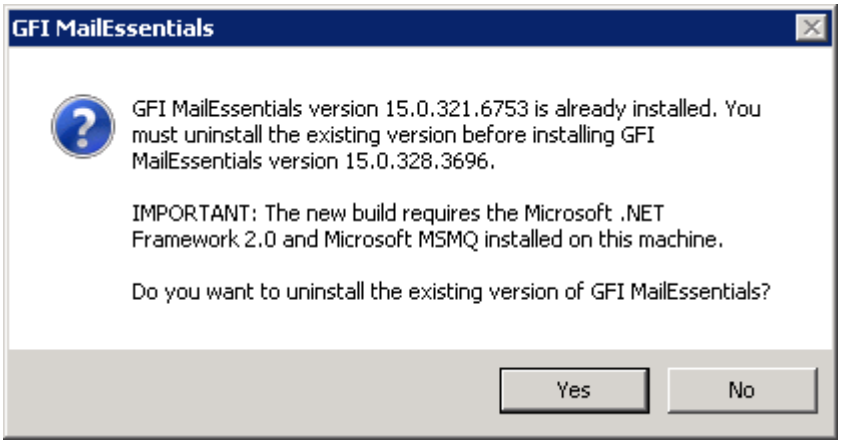
- Upgrades cannot be undone i.e. you cannot downgrade to an

earlier version once you have installed the latest version.

- On upgrading an existing installation, licensing reverts to trial version and a new fully purchased license key for the GFI MailEssentials 2010 is required. For more information on new license keys, refer to: http://customers.gfi.com
- You cannot change the installation path during GFI MailEssentials upgrades.
- When upgrading from GFI MailEssentials 9, the current Bayesian weights file will be upgraded to the new format used in GFI MailEssentials 10 or later. The new format is more compact and uses less memory. NO DATA WILL BE LOST.

Upgrade procedure

1. Launch GFI MailEssentials installation on the server where your earlier version of GFI MailEssentials is installed.


GFI MailEssentials
GFI MailEssentials version 15.0.321.6753 is already installed. You must uninstall the existing version before installing GFI MailEssentials version 15.0.328.3696.
IMPORTANT: The new build requires the Microsoft .NET Framework 2.0 and Microsoft MSMQ installed on this machine.
Do you want to uninstall the existing version of GFI MailEssentials?
Yes
No

Screenshot 75 - Confirm the upgrade

2. Click **Yes** to start the upgrade process and follow on-screen instructions. For assistance refer to New installations section below.

6.4.3 New installations

Important notes

1. During installation, GFI MailEssentials restarts IIS services. This is required to allow GFI MailEssentials components to be registered and started.

2. Before starting installation, close any running Windows applications.

Installation procedure

1. Logon to your Microsoft Exchange Server machine using administrator credentials.

2. Double click **mailessentials2010.exe** (32-bit install) or **mailessentials2010_x64.exe** (64-bit install) accordingly.

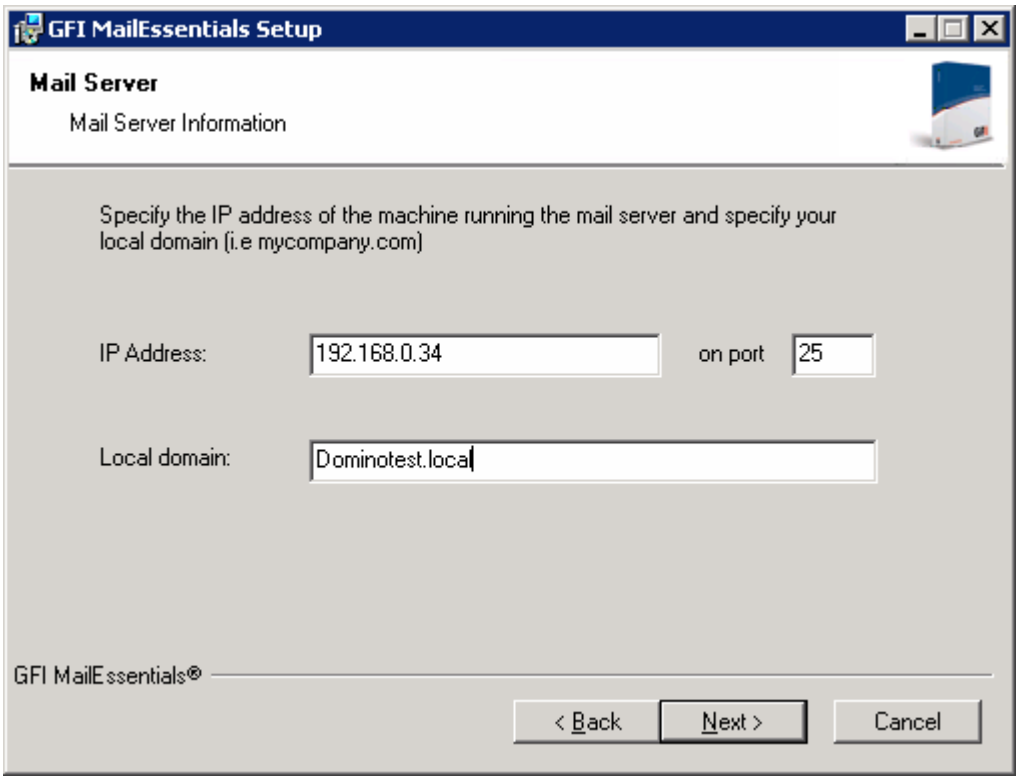
3. Select install language and click **Next**.

4. Select whether to check for newer versions/builds of GFI MailEssentials and click **Next**.

5. Read licensing agreement. To proceed with the installation select **I accept the license agreement** and click **Next**.

6. Click **Next** to install in default location or click **Browse** to change path.

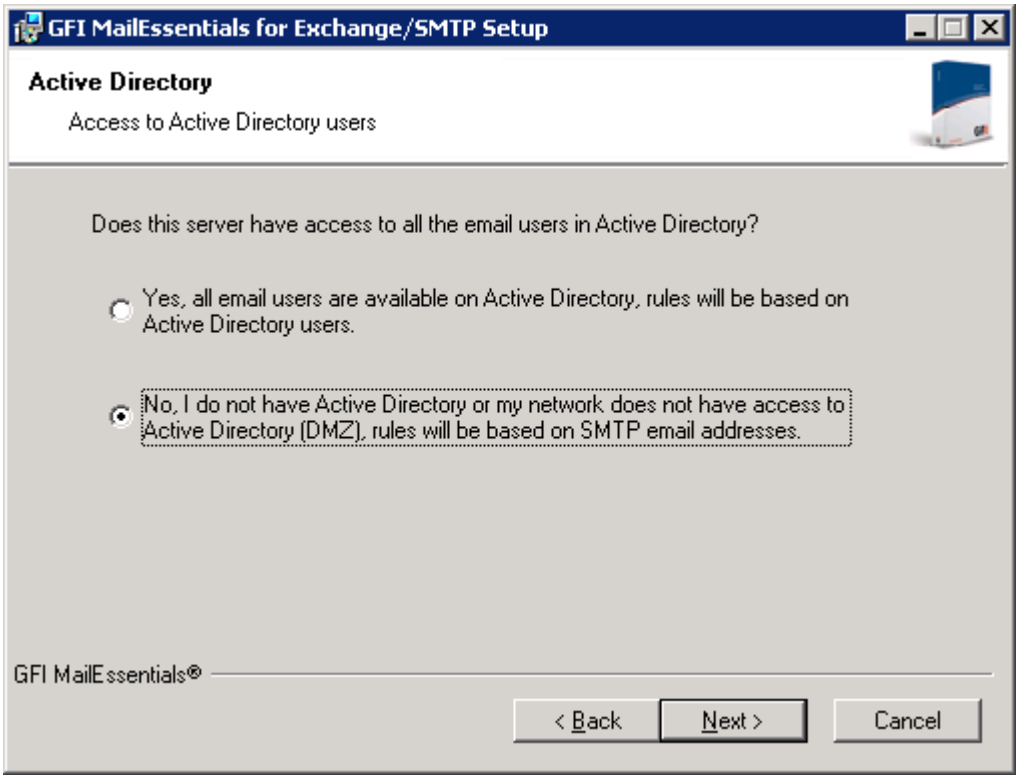
7. Specify user details and enter license key. Click **Next** to continue.



Screenshot 76 - Specify mail server details

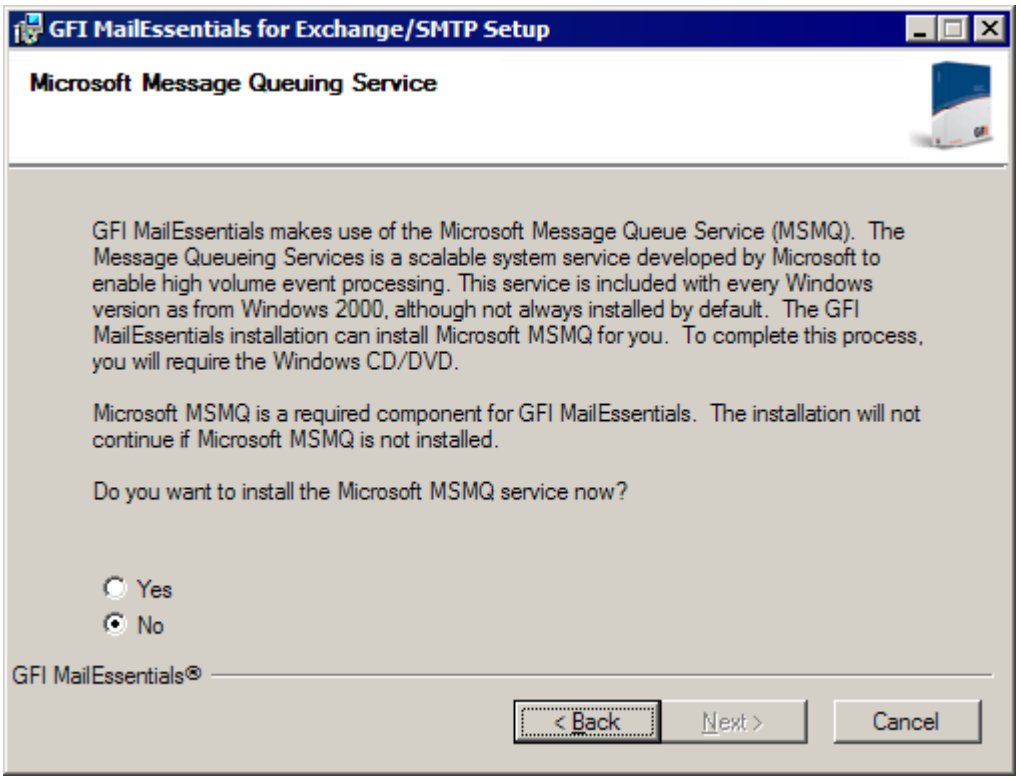
8. Specify IP address and listening port of your SMTP server and the external domain name used. Click **Next** to continue.

9. Specify the email address where notifications (e.g. failed anti spam filters, spam digests) are sent.


GFI MailEssentials for Exchange/SMTP Setup
Active Directory
Access to Active Directory users
Does this server have access to all the email users in Active Directory?
Yes, all email users are available on Active Directory, rules will be based on Active Directory users.
No, I do not have Active Directory or my network does not have access to Active Directory (DMZ), rules will be based on SMTP email addresses.
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 77 - Selecting SMTP mode

10. Select **No, I do not have Active Directory…** option to use SMTP server to get the list of email users. Click **Next** to continue.


GFI MailEssentials for Exchange/SMTP Setup
Microsoft Message Queuing Service
GFI MailEssentials makes use of the Microsoft Message Queue Service (MSMQ). The Message Queueing Services is a scalable system service developed by Microsoft to enable high volume event processing. This service is included with every Windows version as from Windows 2000, although not always installed by default. The GFI MailEssentials installation can install Microsoft MSMQ for you. To complete this process, you will require the Windows CD/DVD.
Microsoft MSMQ is a required component for GFI MailEssentials. The installation will not continue if Microsoft MSMQ is not installed.
Do you want to install the Microsoft MSMQ service now?
Yes
No
GFI MailEssentials®
< Back
Next >
Cancel

Screenshot 78 - Installing Microsoft Message Queuing Service

11. If Microsoft Message Queuing Services (MSMQ) is not installed then the dialog in the above screenshot will open. Select **Yes** to install

MSMQ. Click **Next** to continue.

12. Click **Finish** to finalize your installation. On completion, setup will:

- Ask you to restart the SMTP service.

  IMPORTANT: Failing to restart the SMTP service <u>will negatively affect</u> anti spam filtering and email flow.

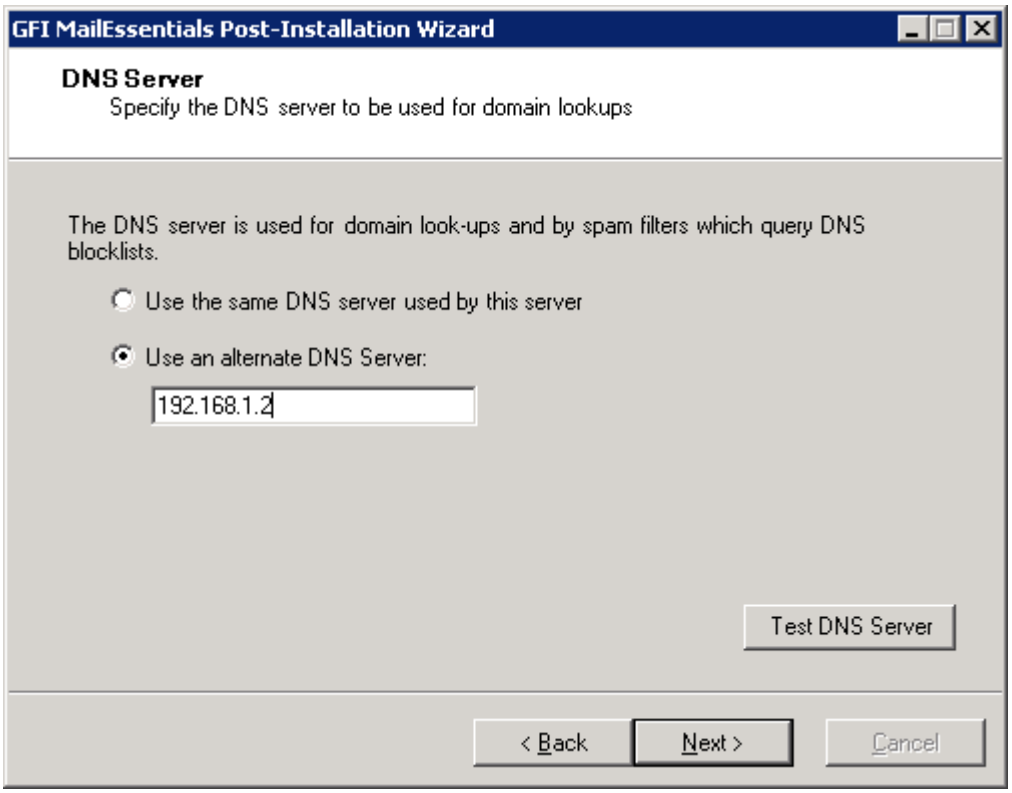
- Check whether Microsoft XML engine is installed. This is automatically installed if not found on UK/US English OS. For other OS languages, this has to be manually downloaded and installed. Microsoft XML engine can be downloaded from:

  http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en

- For new installations, setup will launch the Post-Installation Wizard.

Post-Installation Wizard

1. Click **Next** in the welcome page.

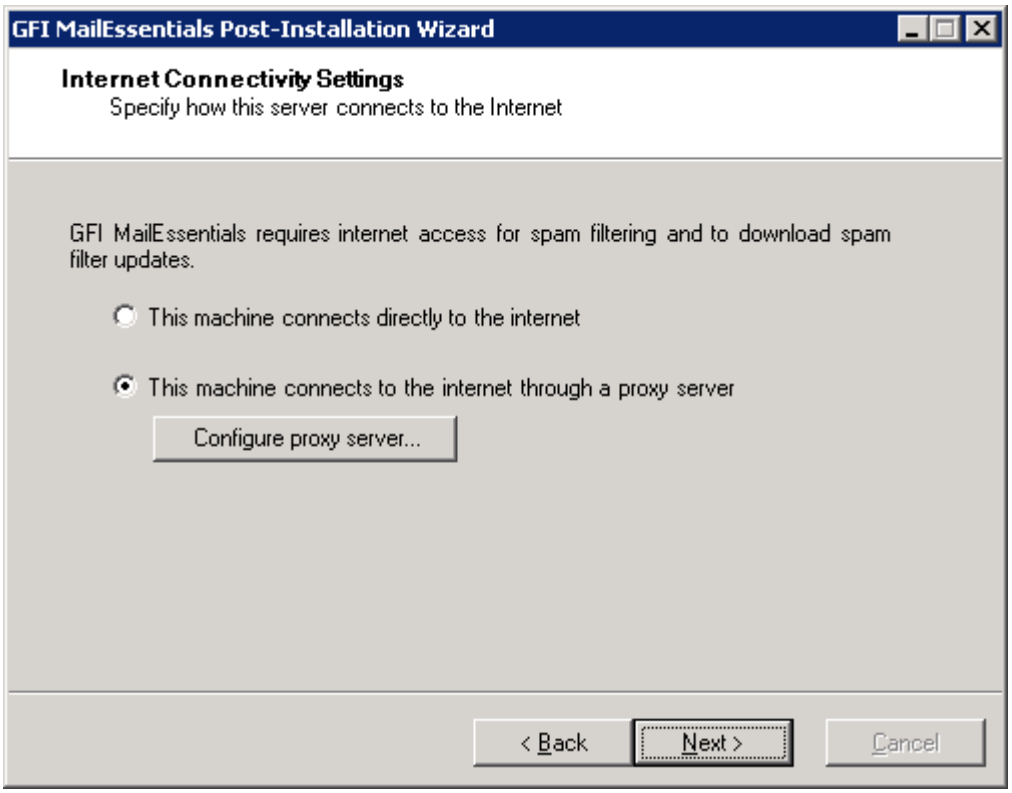

GFI MailEssentials Post-Installation Wizard
DNS Server
Specify the DNS server to be used for domain lookups
The DNS server is used for domain look-ups and by spam filters which query DNS blocklists.
Use the same DNS server used by this server
Use an alternate DNS Server:
192.168.1.2
Test DNS Server
< Back
Next >
Cancel

Screenshot 79 - DNS Server settings

2. In the **DNS Server** dialog, select:

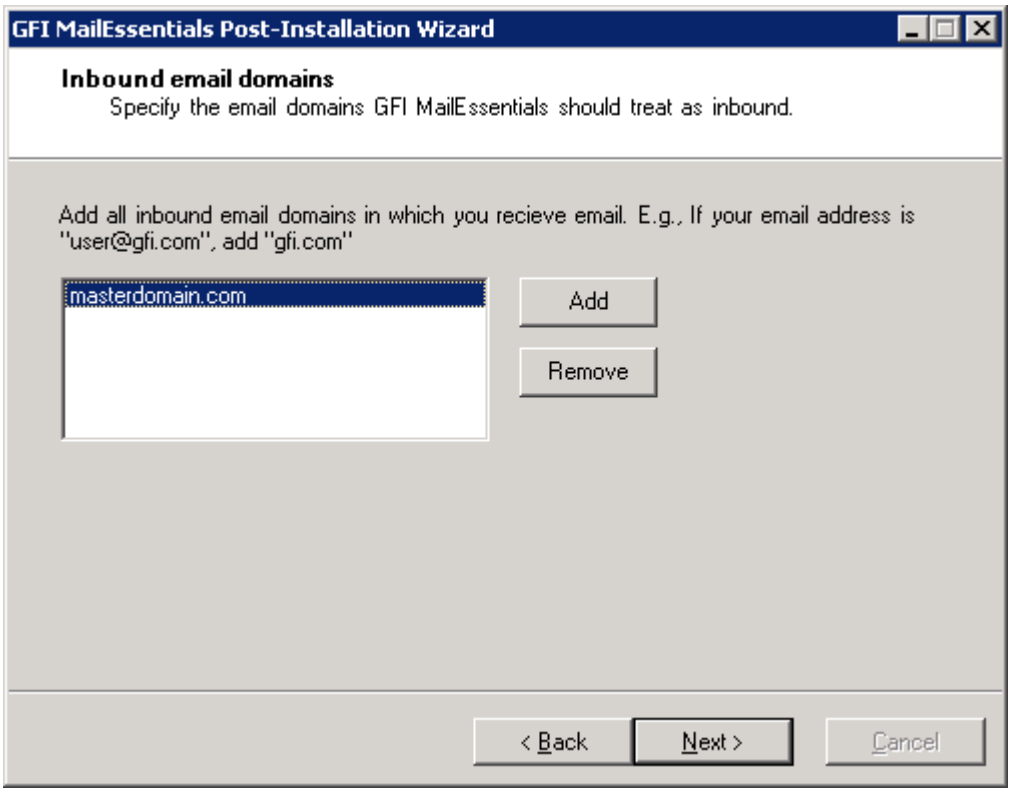
- **Use the same DNS server used by this server** - Select this option to use the same DNS server that is used by the operating system where GFI MailEssentials is installed.
- **Use an alternate DNS server** - Select this option to specify a custom DNS server IP address.

Click **Test DNS Server** to test connection with the specified DNS server. If test is unsuccessful, specify another DNS server. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Internet Connectivity Settings
Specify how this server connects to the Internet
GFI MailEssentials requires internet access for spam filtering and to download spam filter updates.
This machine connects directly to the internet
This machine connects to the internet through a proxy server
Configure proxy server...
< Back
Next >
Cancel

Screenshot 80 - Internet connectivity settings

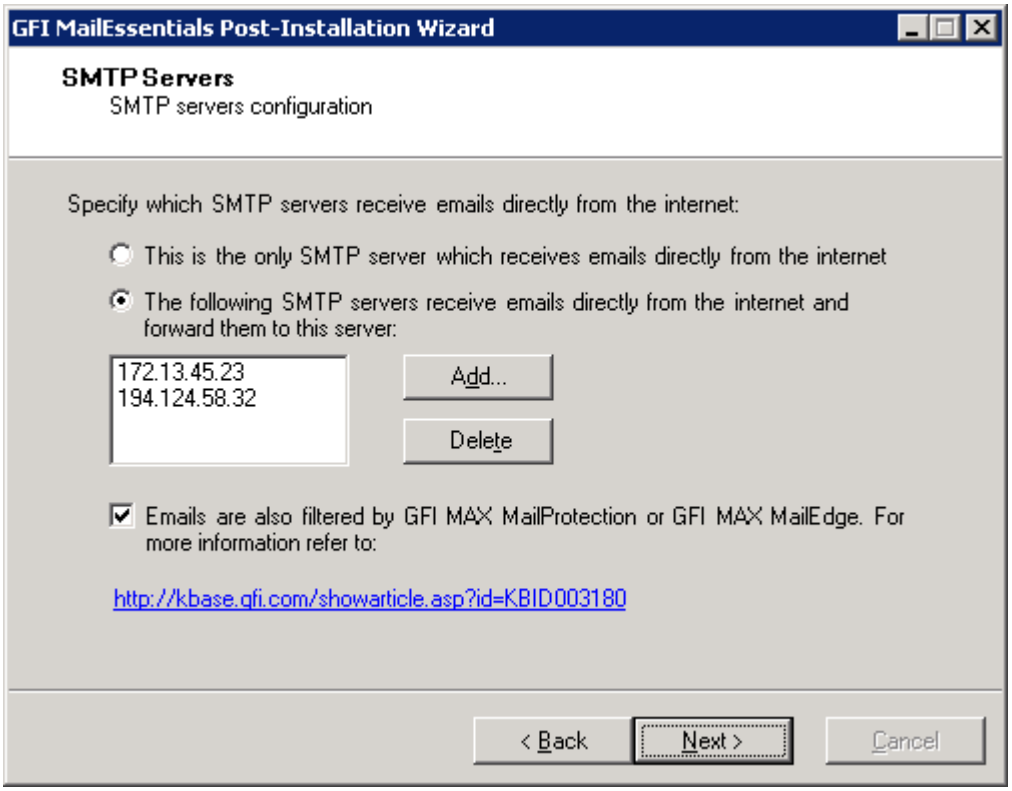
3. In the **Internet Connectivity Settings** dialog, specify how the server where GFI MailEssentials is installed connects to the internet. If the server connects through a proxy server click **Configure proxy server…** and specify proxy settings. Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Inbound email domains
Specify the email domains GFI MailEssentials should treat as inbound.
Add all inbound email domains in which you recieve email. E.g., If your email address is "user@gfi.com", add "gfi.com"
masterdomain.com
Add
Remove
< Back
Next >
Cancel

Screenshot 81 - Inbound email domains

4. In the **Inbound email domains** dialog specify all the domains to filter for spam. Any local domains that are not specified in this list will not be filtered for spam. Click **Next** to continue.

NOTE: When adding domains, select **Obtain domain's MX records and include in perimeter servers list** to retrieve the domain's MX records and automatically add them to the perimeter SMTP servers list (configured in the next step).


GFI MailEssentials Post-Installation Wizard
SMTP Servers
SMTP servers configuration
Specify which SMTP servers receive emails directly from the internet:
This is the only SMTP server which receives emails directly from the internet
The following SMTP servers receive emails directly from the internet and forward them to this server:
172.13.45.23
194.124.58.32
Add...
Delete
Emails are also filtered by GFI MAX MailProtection or GFI MAX MailEdge. For more information refer to:
http://kbase.gfi.com/showarticle.asp?id=KBID003180
< Back
Next >
Cancel

Screenshot 82 - SMTP Server settings

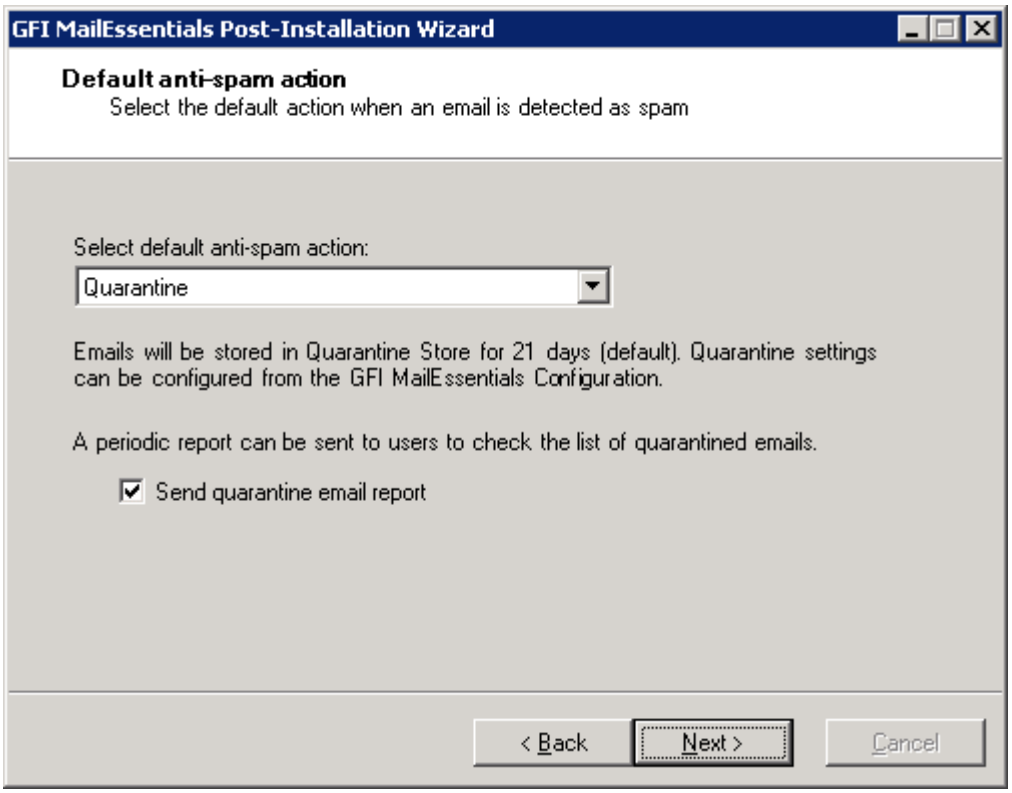
5. In the **SMTP Servers** dialog specify how the server receives external emails. If emails are routed through other servers before they are forwarded to the GFI MailEssentials server, add the IP address of the other servers in the list. For more information about perimeter SMTP servers refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003296

When using hosted email security products GFI MAX MailProtection or GFI MAX MailEdge, enable checkbox **Emails are also filtered by…**. For more information refer to:

http://kbase.gfi.com/showarticle.asp?id=KBID003180

Click **Next** to continue.


GFI MailEssentials Post-Installation Wizard
Default anti-spam action
Select the default action when an email is detected as spam
Select default anti-spam action:
Quarantine
Emails will be stored in Quarantine Store for 21 days (default). Quarantine settings can be configured from the GFI MailEssentials Configuration.
A periodic report can be sent to users to check the list of quarantined emails.
Send quarantine email report
< Back
Next >
Cancel

Screenshot 83 - Selecting the default anti-spam action to use

6. In the **Default anti-spam action** dialog select the default action to be taken when emails are detected as spam. Click **Next** to continue.

7. Click **Finish** to finalize the installation.

The GFI MailEssentials installation is now complete and the anti-spam system is up and running. For more information about how to optimize GFI MailEssentials refer to Post-install actions chapter.

7 Post-install actions

To ensure that your GFI MailEssentials anti spam system is effectively up and running, perform the following post-install actions:

Step 1: Launch GFI MailEssentials Configuration console

Click on **Start ► All Programs ► GFI MailEssentials ► GFI MailEssentials Configuration**.

Step 2: Enable Directory Harvesting

This filter uses Active directory or LDAP lookups to verify whether inbound emails are addressed to legitimate 'internal' email accounts. To enable this filter:

1. Right click **Anti spam ► Anti Spam Filters ► Directory Harvesting** node and select **Properties**.

2. Select **Enable directory harvesting protection**.

3. Select the lookups method to be used:

- **Use native Active Directory lookups option** - Select this option if during installation you selected to get the list of email users from Active Directory (see Installation procedure section above - step 9).
- **Use LDAP lookups** - Select this option if GFI MailEssentials is installed on a server which is not part of your Active Directory domain (e.g. GFI MailEssentials is installed in the DMZ). Directory Harvesting will use LDAP to query Active Directory. (see Installation procedure section above - step 9). In addition:
    - Unselect the **Anonymous bind** option if your LDAP server requires authentication
    - Enter the authentication details using Domain\User format.
    - Click **Test** button to test your LDAP configuration settings.

Step 3: Configure whitelists

This filter allows you to specify lists of 'friendly' email domains, email addresses or IP addresses.

WARNING: USE THIS FEATURE WITH CAUTION. Entries in this list will not be scanned for spam and will bypass all anti spam filtering.

1. Right click **Anti spam ► Whitelist** node and select **Properties.**

2. Click on the **Whitelist** tab.

3. Click **Add…** and specify domains/email addresses or IP addresses to whitelist.

4. Click **OK** to finalize your configuration.

Step 4: Enable Greylist

The Greylist filter temporarily blocks incoming emails received from unknown senders and sends a retry message. A legitimate SMTP server will try to resend an email if a retry message is received, while spam servers normally ignore error messages.

NOTE: To enable Greylist, GFI MailEssentials must be installed on the perimeter SMTP server.

1. Right click **Anti spam ► Anti-Spam Filters ► Greylist** node and select **Properties.**

2. Click the **Greylist** tab.

3. Click **Enable Greylist** to enable Greylist.

4. From the **Email exclusions** and **IP exclusions** tabs specify any email or IP addresses which you do not want to greylist and whether to exclude also whitelisted emails and IP addresses.

5. Click **OK** to finalize your configuration.

7.1 Test your anti spam system

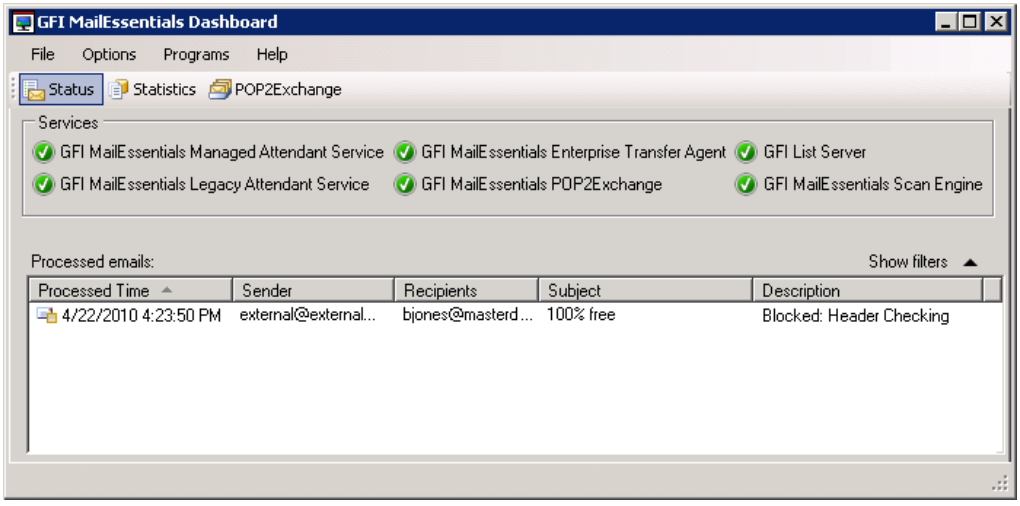
GFI MailEssentials is now ready to start managing spam. To verify that anti spam is working properly:

1. Navigate to **Start ► All Programs ► GFI MailEssentials ► GFI MailEssentials Dashboard**.

2. Using an external email account (for example hotmail or Gmail), create a new email and key in “100% free” as the subject.

3. Send the email to one of your internal email accounts.

4. Allow some time for email delivery and confirm that GFI MailEssentials is working by:



Screenshot 84 - Testing your anti spam system

- Checking the GFI MailEssentials Dashboard. When the email is received, the details are displayed in the MTA logging window. Ensure that the description next to the test email with subject ‘100% free’ is ‘Blocked: Keyword Checking’.
- Verifying that the default anti-spam action chosen was applied (e.g. check if email was delivered to Quarantine).

7.2 GFI MailEssentials Configuration

At this stage, your GFI MailEssentials anti spam system is up and running. All inbound email will be scanned by the anti spam filters enabled by default.

Filter	Description	Enabled by Default
SpamRazer	An anti-spam engine that determines if an email is spam by using email reputation, message fingerprinting and content analysis.	Yes
Directory Harvesting	Stops email which is randomly generated towards a server, mostly addressed to non-existent users.	No
Phishing	Blocks emails that contain links in the message bodies pointing to known phishing sites or if they contain typical phishing keywords.	Yes
Sender Policy Framework	Stops email which is received from domains not authorized in SPF records	No
Auto-Whitelist	Addresses to which an email is sent to, are automatically excluded from being blocked.	Yes
Whitelist	A custom list of safe email addresses	Yes
Email Blocklist	A custom list of blocked email users or domains.	Yes
IP DNS Blocklist	Checks if the email received is from senders that are listed on a public DNS list of known spammers.	Yes
URI DNS Blocklist	Stops emails which contain links to domains listed on public Spam URI Blocklists	Yes
Header checking	A module which detects spam by analyzing the email header.	Yes
Keyword checking	Spam messages are identified based on blocked keywords in the email subject or body	Yes
New Senders	Emails that have been received from senders to whom emails have never been sent before.	No
Bayesian analysis	An anti-spam technique where a statistical probability index based on training from users is used to identify spam.	No
Greylist	Identifies emails received from Non RFC compliant mail servers such as the ones normally used by spammers.	No

The default action taken when an email is classified as spam is configured during the Post-install wizard. Different actions can then be defined for each anti-spam filter.

Filters	Anti spam filter actions						
	Tagging	Quarantine	Delete	Forward to email address	Move to subfolder in user mailbox	Move to junk mail folder	Move to specific folder
SpamRazer	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Directory Harvesting	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Phishing	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sender Policy Framework	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Whitelist	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Email Blocklist	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP DNS Blocklist	Yes	Yes	Yes	Yes	Yes	Yes	Yes
URI DNS Blocklist	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Header checking	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Keyword checking	Yes	Yes	Yes	Yes	Yes	Yes	Yes
New Senders	Yes	Yes	Yes	Yes	Yes	No	Yes
Bayesian analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Greylist	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A - Not applicable

NOTE: The actions for Directory Harvesting are applicable only when Directory Harvesting is executed at full email level.

Configuration of anti spam filters and actions is possible via the GFI MailEssentials Configuration console. For guidelines on how to configure GFI MailEssentials functions and features refer to the GFI MailEssentials Administration and Configuration manual.

8 Uninstalling GFI MailEssentials

8.1 Introduction

This chapter describes how to uninstall GFI MailEssentials for all supported operating systems.

NOTE 1: If you are planning to uninstall and reinstall GFI MailEssentials to fix problems you may be having during installation, you should first read the Troubleshooting and support chapter in this manual.

NOTE 2: Third-party components which are required by GFI MailEssentials, such as Microsoft .NET Framework or Microsoft XML core services, will not be uninstalled.

8.1.1 Uninstall GFI MailEssentials

1. Exit GFI MailEssentials.

2. From the **Control Panel** select:

- **Add or Remove Programs** - Windows Server 2003, Windows SBS 2003.
- **Programs and Features** - Windows Server 2008, Windows SBS 2008/2011.

3. From the list of installed software select **GFI MailEssentials for Exchange/SMTP** and click **Remove** or **Uninstall**.

4. Follow on-screen instructions to uninstall GFI MailEssentials.

9 Troubleshooting and support

9.1 Introduction

This chapter explains how to resolve any GFI MailEssentials issues encountered during installation. The main sources of information available to solve these issues are:

- This manual - most issues can be solved through the information in this manual section.
- GFI Knowledge Base articles
- Web forums
- Contacting GFI Technical Support

9.2 Troubleshooting: Installation issues

Issue	Possible solution
License key for the previous version is not accepted and the upgraded version is in evaluation mode.	When upgrading to a new version of GFI MailEssentials, you are required to upgrade your license key. For more information on how to upgrade your key, refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003408
During installation some errors may be received causing the product not to be installed properly, or not to be installed at all. • Event Type: 'Warning' • Event ID: '0' • Event Source: 'GFI MailEssentials Legacy Attendant Service' • Event Description: 'The GFI MailEssentials Legacy Attendant Service sub-process '8-auantiphish2' has terminated with error code [-1].The sub-process will not be available until the service is restarted. Please contact GFI Support if the problem persists.'	The Microsoft Event log warnings are created due to a missing requirement for the GFI MailEssentials Legacy Attendant service. This requirement is configured by the post-installation wizard and therefore, no warnings of the same type will be reported in the Microsoft event logs after completing the GFI MailEssentials post-installation wizard.
During installation some errors may be received causing the product not to be installed properly, or not to be installed at all. • "Error 1720.There is a problem with this Windows Installer package. • A script required for this	1. Disable any real-time scanning software such as antivirus software. 2. Ensure that you do not have any software that automatically removes files from the TEMP folder. 3. Log in with Domain Administrator privileges. 4. Download and install the latest version of Windows Scripting Host & Windows Installer for your Windows Operating System from: http://www.microsoft.com/downloads/

install to complete could not be run. Contact your support personnel or package vendor.”: • “Setup failed to launch installation engine: Access is denied.” or: • “Error installing Ikernel.exe, access is denied.”	5. Ensure that the following Microsoft Windows technologies are installed correctly and not corrupt: • *Microsoft Windows Management Instrumentation (WMI)* • *Microsoft Windows Installer* • *Microsoft .Net Framework* • *Microsoft Data Access Components (MDAC)* 6. Ensure that the following system libraries located at <Windows\System32> are correctly registered: • *urlmon.dll* • *Oleaut32.dll* • *ole32.dll* • *Actxprxy.dll* • *Shell32.dll* • *Shdocvw.dll* • *Mshtml.dll* • *Browseui.dll* • *Scrrun.dll* To register system libraries perform the following steps: a. Click Start and select Run b. Key in: cmd.exe c. Key in: regsvr32 <path & filename of dll> **Example:** regsvr32 c:\windows\system32\urlmon.dll 7. Place the installation file in a temporary directory on the server where you are installing the GFI product and retry installing GFI MailEssentials. 8. Check Distributed Component Object Model (DCOM) permissions as explained in: http://support.microsoft.com/default.aspx?scid=kb;en-us;295278 **NOTE:** For more information on how to resolve common Windows Installer problems refer to: http://support.microsoft.com/default.aspx?scid=kb;en-us;555175

9.3 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository, which includes answers to the most common installation problems. In case that the information in this manual does not solve your installation problems, next refer to the Knowledge Base. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting:

http://kbase.gfi.com/

9.4 Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting:

http://forums.gfi.com/.

9.5 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form and follow the instructions on this page closely to submit your support request on:

  http://support.gfi.com/supportrequestform.asp

- **Phone:** To obtain the correct technical support phone number for your region please visit:

  http://www.gfi.com/company/contact.htm

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at:

http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

9.6 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:

http://www.gfi.com/pages/productmailing.htm.

9.7 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on:

documentation@gfi.com

10 Appendix - Installing MSMQ

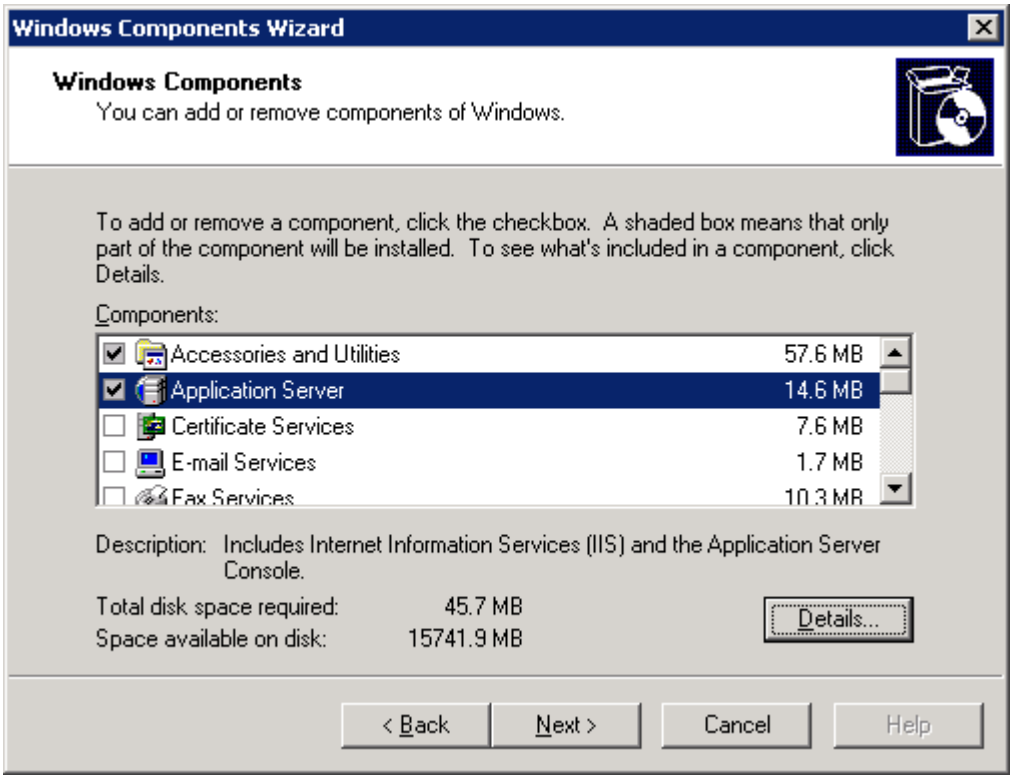
10.1 Windows Server 2003

The message queuing service is a scalable system service developed by Microsoft to enable high volume event processing. GFI MailEssentials uses this service for the list server. The message queuing service is included with every Windows 2003 and XP version, although not always installed by default.

To check whether MSMQ is installed and to install it if it is not:

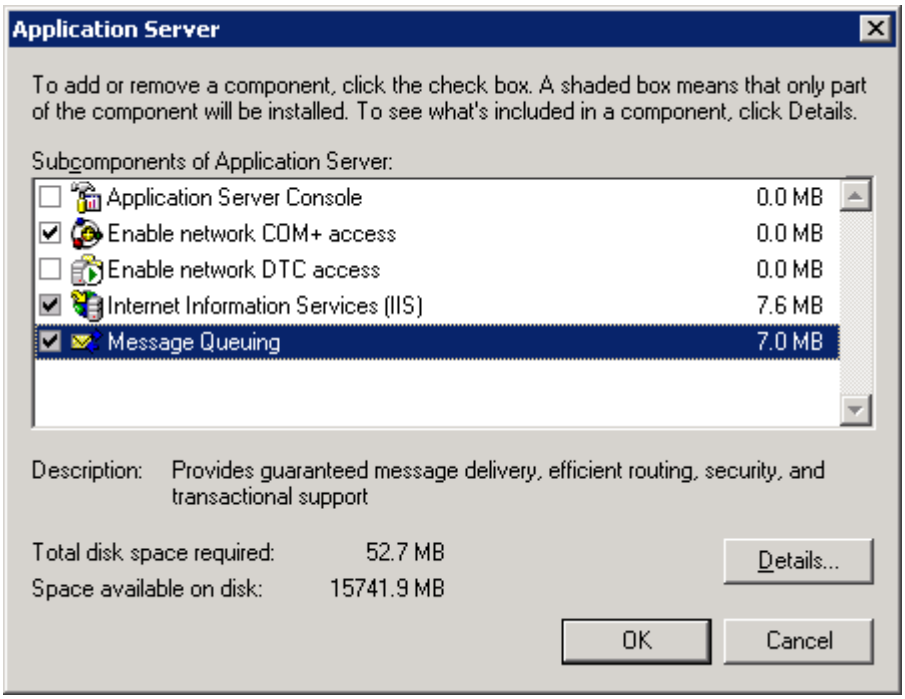
1. Open the Windows Control Panel from the start menu, double-click on Add/Remove Programs and then click on the Windows Components tab to launch and display the Windows components wizard.

2. Click on **Application Server** and then click **Details**.


Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 57.6 MB
Application Server 14.6 MB
Certificate Services 7.6 MB
E-mail Services 1.7 MB
Fax Services 10.3 MB
Description: Includes Internet Information Services (IIS) and the Application Server Console.
Total disk space required: 45.7 MB
Space available on disk: 15741.9 MB
Details...
< Back
Next >
Cancel
Help

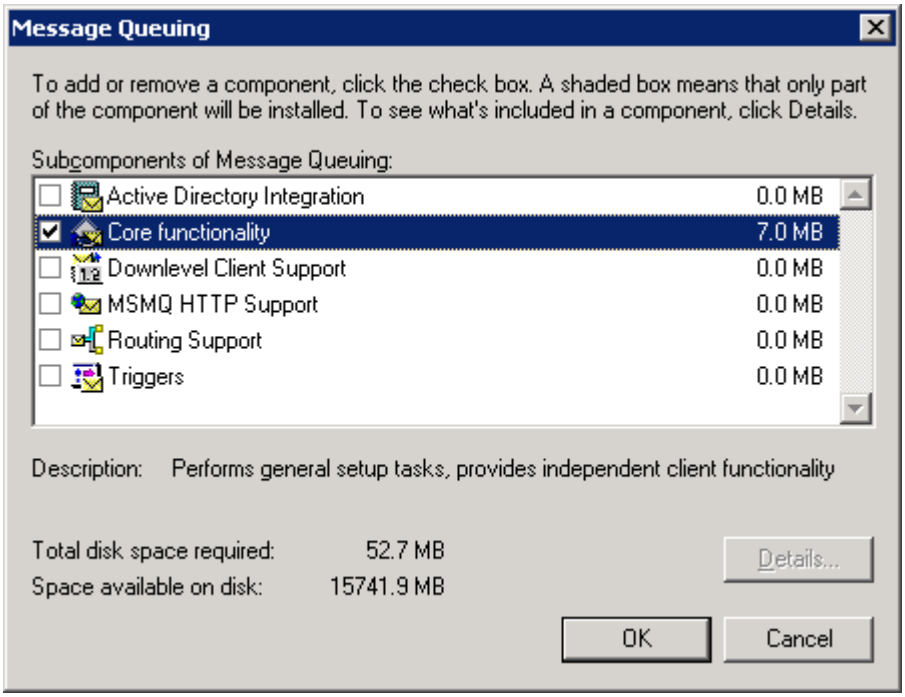
Screenshot 85 - Windows Components Wizard

3. If the **Message Queuing** checkbox is selected it means the service is already installed and you can thus skip the rest of this section. If it is not, then you need to follow the rest of the steps below to install the message queuing service. In the **Application Server** dialog click on **Message Queuing** and then click **Details**.


Application Server
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Application Server:
Application Server Console 0.0 MB
Enable network COM+ access 0.0 MB
Enable network DTC access 0.0 MB
Internet Information Services (IIS) 7.6 MB
Message Queuing 7.0 MB
Description: Provides guaranteed message delivery, efficient routing, security, and transactional support
Total disk space required: 52.7 MB
Space available on disk: 15741.9 MB
Details...
OK
Cancel

Screenshot 86 - Message queuing component

4. In the **Message Queuing** dialog select the **Core functionality** checkbox and then click **OK**.


Message Queuing
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Message Queuing:
Active Directory Integration 0.0 MB
Core functionality 7.0 MB
Downlevel Client Support 0.0 MB
MSMQ HTTP Support 0.0 MB
Routing Support 0.0 MB
Triggers 0.0 MB
Description: Performs general setup tasks, provides independent client functionality
Total disk space required: 52.7 MB
Space available on disk: 15741.9 MB
Details...
OK
Cancel

Screenshot 87 - MSMQ Core functionality

5. In the **Application Server** dialog click **OK** and then click **Next** in the **Windows Components Wizard** window to start installing the message queuing service.

6. When the installation of the message queuing service is complete, you need to click **Finish** in the **Windows Components Wizard**. The Message Queuing Service is now installed.

10.2 Windows Server 2008

For detailed instructions on how to install MSMQ on Windows Server 2008 refer to:

http://technet.microsoft.com/en-us/library/cc730960.aspx

11 Glossary

Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
AD	*See* Active Directory
Auto-reply	An email reply that is sent automatically to incoming emails.
Bayesian Filtering	An anti-spam technique where a statistical probability index based on training from users is used to identify spam.
Background Intelligent Transfer Service	A component of Microsoft Windows operating systems that facilitates transfer of files between systems using idle network bandwidth.
BITS	*See* Background Intelligent Transfer Service
Blocklist	A list of email addresses or domains from whom email is not to be received by users
Botnet	A network of infected computers that run autonomously and are controlled by a hacker/cracker.
CIDR	*See* Classless Inter-Domain Routing
Classless Inter-Domain Routing	An IP addressing notation that defines a range of IP addresses.
Demilitarized Zone	A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.
Disclaimer	A statement intended to identify or limit the range of rights and obligations for email recipients
Domain Name System	A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.
DMZ	*See* Demilitarized Zone
DNS	*See* Domain Name System
DNS MX	*See* Mail Exchange
Email monitoring rules	Rules which enable the replication of emails between email addresses.
False negatives	Spam emails that are not detected as spam.
False positives	Legitimate emails that are incorrectly identified as spam.
Greylist filter	An anti-spam filter that blocks emails sent from spammers that do not resend a message when a retry message is received.
Ham	Legitimate e-mail
IIS	*See* Internet Information Services

Internet Information Services	A set of Internet-based services created by Microsoft Corporation for internet servers.
IMAP	*See* Internet Message Access Protocol
Internet Message Access Protocol	One of the two most commonly used Internet standard protocols for e-mail retrieval, the other being POP3.
LDAP	*See* Lightweight Directory Access Protocol
Lightweight Directory Access Protocol	An application protocol used to query and modify directory services running over TCP/IP
List server	A server that distributes emails sent to discussions lists and newsletter lists, and manages subscription requests.
Mail Exchange	The DNS record used to identify the IP addresses of the domain's mail servers.
MAPI	*See* Messaging Application Programming Interface
MDAC	*See* Microsoft Data Access Components
Messaging Application Programming Interface	A messaging architecture and a Component Object Model based API for Microsoft Exchange.
Microsoft Message Queuing Services	A message queue implementation for Windows Server operating systems.
Microsoft Data Access Components	A Microsoft technology that gives developers a homogeneous and consistent way of developing software that can access almost any data store.
MIME	*See* Multipurpose Internet Mail Extensions
MSMQ	*See* Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	A standard that extends the format of e-mail to support text other than ASCII, non-text attachments, message bodies with multiple parts and header information in non-ASCII character sets.
NDR	*See* Non Delivery Report
Non Delivery Report	An automated electronic mail message sent to the sender on an email delivery problem.
Perimeter server/gateway	The computer (server) in a LAN that is directly connected to an external network. In GFI MailEssentials perimeter gateway refers to the email servers within the company that first receive email from external domains.
Phishing	The process of acquiring sensitive personal information with the aim of defrauding individuals, typically through the use of fake communications
POP2Exchange	A system that collects email messages from POP3 mailboxes and routes them to mail server.
POP3	*See* Post Office Protocol ver.3
Post Office Protocol ver.3	A protocol used by local email clients to retrieve emails from mailboxes over a TCP/IP connection.
Public folder	A common folder that allows Microsoft Exchange user to share information.
Quarantine	A database where all inbound emails detected as spam are retained for a number of days
RBL	*See* Realtime Blocklist
Realtime Blocklist	Online databases of spam IP addresses. Incoming emails are compared to these lists to determine if they are originating from blocked users.

Remote commands	Instructions that facilitate the possibility of executing tasks remotely.
Secure Sockets Layer	A protocol to ensure an integral and secure communication between networks.
Simple Mail Transport Protocol	An internet standard used for email transmission across IP networks.
SMTP	*See* Simple Mail Transport Protocol
Spam actions	Actions taken on spam emails received, e.g. delete email or send to Junk email folder.
SSL	*See* Secure Sockets Layer
WebDAV	A HTTP extensions database that enables users to manage files remotely and interactively. Used for managing emails in the mailbox and in the public folder in Microsoft Exchange.
Whitelist	A list of email addresses and domains from which emails are always received
Zombie	An infected computer that is part of a Botnet.

12 Index

A

Active Directory, 7, 9, 15, 23, 31, 37, 47, 49, 58, 76, 99, 113

Antivirus, 6, 46, 68, 84, 105

Auto-replies, 3

B

Bayesian Analysis, 101

C

Cluster, 6, 28, 29, 30, 31, 36, 42, 43, 64

D

Dashboard, 100

Directory harvesting, 3, 99, 101, 102

Disclaimers, 9, 23, 37, 58, 83

DMZ, 5, 15, 16, 47, 99, 113

DNS Server, 22, 88

E

Email Blocklist, 101

Email monitoring, 3

G

GFI MailEssentials reporter, 6

Greylist, 3, 100, 102, 113

H

Header checking, 7, 68, 101

I

IIS SMTP, 16, 17, 22, 56, 69, 73, 85, 89

IMAP, 114

Inbound mail filtering, 3

Internal email, 22, 73, 100

IP DNS Blocklist, 7, 68, 101

K

Keyword checking, 100, 102

L

LDAP lookups, 16, 99

Legitimate email, 113

Licensing, 2, 8, 15, 29, 36, 47, 57, 74, 90

Lotus Domino, 67, 69, 72, 73

M

MAPI, 46, 114

Microsoft Exchange Server, 5, 8, 15, 18, 23, 45, 48, 54, 55, 56, 57, 70

MSMQ, 10, 24, 32, 38, 50, 59, 77, 92, 109, 111, 114

N

New Senders, 3, 101, 102

Newsletter, 114

O

Outbound mail filtering, 4

P

perimeter server, 1, 5, 15, 45, 54, 114

Phishing, 7, 68, 101, 114

POP2Exchange, 29, 114

POP3, 114

Q

Quarantine, 6, 100

R

Remote commands, 4, 115

S

Sender Policy Framework, 7, 68, 101

SMTP Server, 9, 16, 17, 23, 37, 49, 58, 69, 70, 83, 85, 86, 88, 92, 100

SMTP Virtual Server, 17, 18, 70, 86, 87

Spam actions, 115

SpamRazer, 7, 68, 101

U

Updates, 7, 68

URI DNS Blocklist, 101

W

WebDAV, 115

Whitelist, 4, 99, 101